A NEW METHOD FOR GEOMETRIC INTERPRETATION OF ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM

Daniele Di Tullio [1] & Ankan Pal [2]
[1] Department of Mathematics, Roma Tre, Italy
[2] Department of Mathematics, University of L'Aquila, Italy
E-mail: danieleditullio@hotmail.it [1]
ankanpal100@gmail.com [2]

Abstract: In this paper, we intend to study the geometric meaning of the discrete logarithm problem defined over an Elliptic Curve. The key idea is to reduce the Elliptic Curve Discrete Logarithm Problem (EC-DLP) into a system of equations. These equations arise from the interesection of quadric hypersurfaces in an affine space of lower dimension. In cryptography, this interpretation can be used to design attacks on EC-DLP. Presently, the best known attack algorithm having a sub-exponential time complexity is through the implementation of Summation Polynomials and Weil Descent. It is expected that the proposed geometric interpretation can result in faster reduction of the problem into a system of equations. These overdetermined system of equations are hard to solve. We have used F4 (Faugere) algorithms and got results for primes less than 500,000. Quantum Algorithms can expedite the process of solving these over-determined system of equations. In the absence of fast algorithms for computing summation polynomials, we expect that this could be an alternative. We do not claim that the proposed algorithm would be faster than Shor's algorithm for breaking EC-DLP but this interpretation could be a candidate as an alternative to the 'summation polynomial attack' in the post-quantum era.

Key Words: Elliptic Curve Discrete Logarithm Problem, Intersection of Curves, Grobner Basis, Vanishing Ideals.

1. INTRODUCTION

Elliptic curves defined over a finite field ($E(\mathbb{F}_p)$) essentially are rich mathematical structures which result in their ubiquitous use in Number Theory, Cryptography, and Algebraic Geometry. EC-DLP has myriad applications and it is used to design most of the classical crypto-systems involving Elliptic Curves. Initially, index calculus methods were used to attack the EC-DLP. The major impediment to such attacks was to find a computationally optimized factor base $\mathcal{F}$. There were considerable improvements in this direction using baby-step-giant-step method. In the case, in which the cardinality of the set of the rational points is a smooth number the

Pohlig-Hellman attack [1] is quite efficient. Pollard's ρ and λ methods were another approach for designing the attacks [2]. The case for supersingular elliptic curves was solved by the use of Weil Paring (MOV Attacks) [3]. The case for curves of cardinality p (trace = 1) is easily reduced to DLP over $\mathbb{Z}/p\mathbb{Z}$. In the other cases the EC-DLP is still hard to attack. Presently, the best method known attack algorithm having a sub-exponential time complexity for particular cases is through the implementation of Summation Polynomials and Weil Descent [4] [5] [6].

In 2000, approaches which use tools from Algebraic Geometry were presented for EC-DLP by Galbraith and Smart [4]. In this paper, Weil descent was used to attack EC-DLP. The use of Weil restrictions, modified the problem of solving EC-DLP on the elliptic curve defined over a finite field extension to solving it on the jacobian of a higher genus curve but defined over a smaller base field [7]. Sub-exponential time algorithms exists for solving the EC-DLP over higher genus curves [8]. This was an approach which was successful for many particular cases. In his seminal paper of 2004, Semaev [5] constructed summation polynomials to solve EC-DLP. Grobner basis was used for solving the system of equations that arose from such problems. A working attack algorithm of sub-exponential time complexity for small dimensions was developed by Gaudry [7] using the concepts of Summation Polynomials and Weil Restrictions.

Solving EC-DLP generally does not have fast algorithms. All the existing methods rely heavily on computing the summation polynomials. This reliance is avoided and a new method for attacking EC-DLP is elucidated. The major drawback of the intersection method is that it produces over-determined system of equations which have high time complexity. We have used Grobner basis and F4 (Faugre) algorithm [9] to solve these system of equation. This has not produced good results for large primes (the characteristic of the base field). For primes less than 500,000, the intersection method produces good result. We have implemented the intersection method with the help of MAGMA [10]. In the post quantum era, we expect that we can solve the system of equations using the methods as illustrated in [11] [12] [13]. We do not expect that the intersection method would be an alternative to Shor's algorithm for solving EC-DLP [14] in the post-quantum paradigm. Nonetheless, we propose the intersection method as an alternative to the 'summation polynomial' attack. The reason for such a tentative claim is straight-forward and it stems from the fact that there are no quantum algorithms for computing summation polynomials in an efficient way.

2. Intersection of Curve Method

Let, $E(\mathbb{F}_q)$ be an Elliptic Curve defined over a finite field of order q where q is a prime power, for some prime p. $P, Q \in E(\mathbb{F}_q)$ and $n \in \mathbb{Z}/N\mathbb{Z}$ and $N = ord(P)$. We can define the EC-DLP in this setting as:

$$Q = nP$$

, where $n < \#E(\mathbb{F}_q)$ By Hasse's Theorem we have that $\#E(\mathbb{F}_q) \sim q$. The order of P is known, since it can be quite efficiently computed by the SEA algorithm. Let, $m = \lfloor \log_2(N) \rfloor$. Now, we can express n as:

$$n = \sum_{i=0}^{m} \epsilon_i 2^i \qquad \epsilon_i \in \{0, 1\}$$

Then, we define P_i as:

$$P_i := 2^i P \qquad \forall i = 0, ..., m$$

It follows that:

$$Q = \sum_{i=0}^{m} \epsilon_i P_i$$

Let $K(E)$ be the set of all rational functions. Note that if we are able to find a function $f \in K(E)$ such that the support of $\operatorname{div}(f)$ is contained in $\{P_0, ..., P_m, -Q, \mathcal{O}\}$, then we are able to find a relation among P and Q. This is the idea of our geometric approach for solving the DLP. To illustrate this fact we provide a well known theorem from basic algebraic geometry:

Theorem A [15]: Let X be an affine variety. Then a rational function which is regular at all points of X can be described as a polynomial function.

Proposition: Let, $C : f(x, y) = 0$ be an affine curve and $r(x) := \operatorname{Res}_y(f(x, y), y^2 - (x^3 + Ax + B))$ and $P_0 = (x_0, y_0) \in E$. Then:

$$v_{(x-x_0)}(r(x)) = (C \cdot E)_{P_0} + (C \cdot E)_{-P_0}$$

Proof: It is a 2-step proof:

Step 1: To reduce the proposition to the case where there are no points of $C \cap E$ on the same vertical line ($x = x_i$)

(Step 2): Now we prove that:

$$v_{x-x_0}(r(x)) = (C \cdot E)_{P_0}$$

Proof of Step 1:

Let, P_0 and $-P_0 \in C \cup E$

Then considering $\dfrac{f(x,y)}{x - x_0}$ is regular on the affine part of E. Therefore, $\exists$ a polynomial $g(x,y)$ such that $g(x,y) = \dfrac{f(x,y)}{x - x_0}$ on $E(\overline{\mathbb{F}}_q)$ or equivalently $f(x,y) = (x - x_0)g(x,y) \pmod E$ [Invoking Theorem A]. The resultant is multiplicative and from the above argument, it follows that:

$$\mathrm{Res}_y(E, f(x,y)) = \mathrm{Res}_y(E, x - x_0)\mathrm{Res}_y(E, g(x,y))$$

$$\mathrm{Res}_y(E, f(x,y)) = (x - x_0)^2\mathrm{Res}_y(E, g(x,y))$$

Iterating the process we get the reduction which proves our assertion for the first step.

Proof of Step 2:

Now, we can safely assume that there are no points of $C \cap E$ in the same vertical line. Hence, the assertion becomes:

$$v_{x-x_0}(r(x)) = (C \cdot E)_{P_0}$$

We observe that if all the points are simple then the 'Resultant' is a square-free polynomial which is given by:

$$\prod_{P \in C \cap E} (x - x_P)$$

(Where all the x_p are different)

Let's consider the case where we have a tangent (T_{P_0}) at P_0 then:

$$v_{x-x_0} = (\mathrm{Res}_y(E, T_{P_0})) = 2 \ or \ 3$$

(Depends if the point is a flex or not!)

We prove the step 2 by induction on:

$$M = \sum_{P \in C \cap E} (C \cdot E)_P - 1$$

If, $M = 0$ then the points are simple. Let's suppose that $M > 0$, and let P_0 be a point such that the $(C \cdot E)_{P_0} \geq 2$. Then, considering $\dfrac{f(x,y)}{T_{P_0}}$ we have 3 possibilities:

1) Considering P_0 is not a flex. If, all the points of intersection belong to $C \cap E$ and P_0 is not a flex. Then, $\dfrac{f(x,y)}{T_{P_0}}$ is a regular function. Hence, by

the previous argument we can reduce M and apply induction accordingly to deduce the result.

2) If P_0 is not a flex but we have a third point of intersection (R) $\notin$ $C \cap E$. Then, considering a line L_R passing through R and through other two points whose x-coordinates are different from each other and also different from that of the points in $C \cap E$. Now, we deduce that $\left(\dfrac{f(x,y)}{T_{P_0}}\right)(L_R)$ is regular and the value of M for the divisor associated to this function has reduced.

3) If P_0 is a flex. Then, we have 2 sub-cases:

3a) $$(C \cdot E)_{P_0} \geq 3$$

In this case, it is a straightforward deduction that $\dfrac{f(x,y)}{T_{P_0}}$ is regular in the affine part of E and in this way we have reduced the value of M and apply induction accordingly to deduce the result.

3b) $$(C \cdot E)_{P_0} = 2$$

For this case we consider a line passing through P_0 and other two points whose x-coordinates are different from each other and also different from that of the points in $C \cap E$. Now, we deduce that $\left(\dfrac{f(x,y)}{T_{P_0}}\right)(L_{P_0})$ is regular and the value of M for the divisor associated to this function has reduced.

This ends the proof of the proposition. We continue with the explanation of the intersection method.

Suppose that the solution n to the DLP is even and let:

$$\frac{n}{2} = \sum_{i=0}^{m-1} \varepsilon_i \cdot 2^i$$

This is the base 2 decomposition. Note that this is not a huge restriction as the algorithm can check for $P = (n-1)Q$ in case we do not find an even n. Now, we recall the group isomorphim:

$$E \rightarrow Pic^0(E)$$

$$P \mapsto (P) - (O)$$

Here, we want to highlight that in $Pic^0(E)$ we can view the EC-DLP in terms of divisors. The idea here is to use the concept of principal divisors which enables us to write the relations of the following form:

$$\sum_i P_i = O$$

Hence, we can be sure that we can write these relationships in terms of the existence of polynomial functions $f(x, y)$ on E such that the $\text{div}(f) = \sum_i (P_i) - (O)$ in the group of divisors which implies that the restriction to the affine part of E is equal to $\sum_i (P_i)$. Since, $n = \sum_{i=0}^{m-1} 2\varepsilon_i \cdot 2^i$. We have that there exists a function $f(x, y) \in K(E)$ and regular in the affine part of E, such that:

$$\text{div}(f) = (-2m - 1)(O) + (-Q) + \sum_{i=0}^{m-1} (1 + \varepsilon_i)(P_i) + (1 - \varepsilon_i)(-P_i)$$

Note that, by the previous proposition we have that:

$$\text{Res}_y(f(x, y), y^2 - (x^3 + Ax + B)) = (x - x_0)^2 \cdots (x - x_{m-1})^2 (x - x_Q)$$

Where, $P_i = (x_i, y_i)$, $Q = (x_Q, -y_Q)$. Since, f is regular in the affine part of E, it is an element of $\mathbb{F}_q[x, y]/(y^2 - (x^3 + Ax + B))$, which is uniquely determined by a polynomial of the form:

$$f(x, y) = yg(x) + h(x)$$

Let, $d = \deg(f(x, y)) = d$, we can write:

$$g(x) = g_0 + \ldots + g_{d-1}x^{d-1}$$

$$h(x) = h_0 + \ldots + h_d x^d$$

Hence, the functions which are regular on the affine part can be parametrized up to constant by a projective space $\mathbb{P}^{2d}$. The resultant can be expressed (up to multiplication by a non-zero constant) in the following way:

$$r(x) = (h(x))^2 - (g(x))^2(x^3 + Ax + B)$$

So, if $g_{d-1} \neq 0$ and $r(x)$ is an uni-variate polynomial of degree $2d + 1$. It follows that imposing $d = m$, $g_{d-1} = 1$ and that:

$$r(x) = (x - x_0)^2 \cdots (x - x_{m-1})^2 (x - x_Q)$$

We are imposing the condition that, $2m + 1 = 2d + 1$ algebraic conditions (more precisely quadratic conditions) on an affine space of dimension $2m$. Let, $I \triangleleft \kappa[g_0, \ldots, g_{d-2}, h_0, \ldots, h_d]$ be the ideal generated by these equations. This results in an over-determined system which has no solution, in general. This is not surprising, since in general there is no solution for the EC-DLP. The Diffie-Helmann Key exchange which is the basic example of posing EC-DLP would not be possible if there is no solution. Hence, it can be safely assumed that for such a system for specific/recommended curves will have solution. But if there is a solution, then they are at least 2, in fact:

$$(g_0, \ldots, g_{d-2}, h_0, \ldots, h_d) \in V(I) \iff (g_0, \ldots, g_{d-2}, -h_0, \ldots, -h_d) \in V(I)$$

This corresponds to the fact that if:

$$Q = \sum_{i=0}^{m-1}[2\varepsilon_i]P_i \iff -Q = \sum_{i=0}^{m-1}[-2\varepsilon_i]P_i$$

In general, there can be also more solutions if we do not require that $f(P_i) = 0$ and $f(-Q) = 0$, which are $m + 1 = d + 1$ linear conditions on the coefficients of f. So, at the end we have a variety in $\mathbb{A}^{2d}_{\overline{\mathbb{F}_q}}$ defined by $d + 1$ linear equations and $2d + 1$ quadratic equations. Note that some of the quadratic conditions are redundant. One of the instances is the condition $f(x_i, y_i) = 0$ and $r(x_Q) = 0$ which imply that $r(x_i) = 0$ and $r(x_Q) = 0$. Therefore, there are $d + 1$ linear conditions and d independent quadratic conditions given by:

$$r'(x_i) = 0, \qquad \forall\, i \in \{0, ..., m - 1\}$$

Thus, essentially we are studying the zero set of the interesection of d quadric hypersurfaces in an affine space of dimension $d - 1$.

Remark: Note that if $Order(P)$ is even and n is odd this algorithm produces *no solution*. Instead if n is even then there can be two solutions if $n + Order(P)$ has the same binary length of $Order(P)$. If $Order(P)$ is odd (it is very common that $\#E(\mathbb{F}_p)$) is chosen to be a prime number for security reasons) then there is a unique solution provided n is even. If n is *odd* there is exactly 1 solution corresponding to $n + Order(P)$ if this number has the same binary length of $Order(P)$, no solutions otherwise.

3. Algorithm

The algorithm consists of steps which depends on accessing the points on the elliptic curve and operating on them to implement the idea of intersection of surfaces. It starts with initialization of the finite field and the elliptic curve defined over it. Then we generate a polynomial ring and define the required polynomials. The vanishing ideals are evaluated henceforth and the derivative is computed. After this Grobner basis is computed and the F4 algorithm is implemented to solve the system of equations. The algorithm is realized through MAGMA. One can find the MAGMA code here. We would like to emphasize that we have not implemented '*any*' quantum algorithm. The implementation is purely classical. We hereby provide the pseudocode for the the sub-routines of the algorithm.

Algorithm 1: Intersection Method

---

1 construct FiniteField(p,k), EllipticCurve([F | A,B]) and $P \in E$ /* p is a prime number and A,
   B are the coefficients of the elliptic curve equation   */
2 **for** $s = 0;\ s < m_1;\ s = s + 1$ **do**
3 $\quad$ define ps as $[2^s * P]$
4 **end**
   /* Operation on the point P. $m = Floor(Log(2, n)), m_1 = m - 1, m_2 = m - 2$ and similarly
      we can continue   */
5 construct PolynomialRing(F, $2 * m$) (R) and PolynomialRing(R, 2) /* The variable is w and k
      respetively   */
6 **for** $i = 1;\ i < m;\ i = i + 1$ **do**
7 $\quad$ define h as w[i]
8 **end**
   /* Array of coefficients   */
9 construct Polynomial(h) (H) and Polynomial(g) (G) /* Variables are u and v respectively
      */
10 Evaluate(H, k[1]) and Evaluate(G, k[1]) + $k[1]^{(m_2)}$ /* Evaluating the Polynomial   */
11 **for** $i = 1;\ i < (\#T + 1);\ i = i + 1$ **do**
12 $\quad$ define Z as [Evaluate(f, T[i])]
13 **end**
   /* Array ps is called and an array of arrays is constructed and named T. f is
      defined as the addition of the evaluation in previous steps   */
14 construct an ideal i_1 as $< R\ |\ Z >$ /* Initializing the ideal for calculating the
      vanishing ideal. i_2, i_3, i_4, i_5 ideals are constructed consequently   */
15 Evaluate Derivative(r, k[1]) /* r is $x1^2 - k[1]^3 * y1^2 - A * k[1] * y1^2 - B * y1^2$ */
16 initialize Q as $(n - 100) * P$
17 compute Radical(i_5), Groebner(R), PrimaryDecomposition(R), GroebnerBasis(R[1])
18 **for** $i = 1;\ i < (\#Z + 1);\ i = i + 1$ **do**
19 $\quad$ **if** $Z[i] = 0$ **then**
20 $\quad\quad$ Set $Z_1 = [0]$
21 $\quad$ **end**
22 $\quad$ **else**
23 $\quad\quad$ set $Z_1 = [\ Z[i]\ ]$
24 $\quad$ **end**
25 **end**
   /* Z is constructed as the array of arrays of the primary decomposition   */
26 **for** $i = 1;\ i < (\#Z + 1);\ i = i + 1$ **do**
27 $\quad$ **if** $Z_1[i] = 0$ **then**
28 $\quad\quad$ set $Z_2 = [0]$
29 $\quad$ **end**
30 $\quad$ **else**
31 $\quad\quad$ set $Z_2 = [\ 2^{(Z_1[i])}\ ]$
32 $\quad$ **end**
33 **end**

---

4. Conclusion and Future Work

The complexity of the curve intersection algorithm depends majorly on finding the vanishing ideals and the system of equations which are over-determined in nature. Hence, using classical tools and technique, the complexity is quite high. As we have highlighted that the proposed method

produces overdetermined system of equations which are hard to solve. In the classical paradigm, machine learning technique gives us hope to solve these kind of system with a comparatively lower (probabilistic) time complexity. Another approach which is worth exploring is Zhuang-Zi [16] which provides a new technique to solve system of multivariate polynomial equations over a finite field. In the post quantum paradigm, efficient methods for solving these system of equations are illustrated in [11] (only for boolean case), and [13] (linear system of equations). [12] entails a quantum algorithm for solving non linear system of equations in $GF(q = p^k)$ which might be used for improving the proposed method in the future. We reiterate that *we do not expect that the intersection method would be an alternative to Shor's algorithm for solving EC-DLP* [14] in the post-quantum paradigm. Nonetheless, we propose the intersection method as an alternative to the 'summation polynomial' attack. The reason for such a tentative claim is straight-forward and it stems from the heuristics that the proposed method is fast in reducing EC-DLP into a over-determined system of equations which we expect to be solved efficiently by a quantum computer.

5. Acknowledgements

References

[1] Washington, L.C., 2008. Elliptic curves: number theory and cryptography. Chapman and Hall/CRC.

[2] Pollard, J.M., 1978. Monte Carlo methods for index computation (mod p) Mathematics of computation, 32(143), pp.918-924.

[3] Menezes, A.J., Okamoto, T. and Vanstone, S.A., 1993. Reducing elliptic curve logarithms to logarithms in a finite field. iEEE Transactions on information Theory, 39(5), pp.1639-1646.

[4] Galbraith, S.D. and Smart, N.P., 1999, December. A cryptographic application of Weil descent. In IMA International Conference on Cryptography and Coding (pp. 191-200). Springer, Berlin, Heidelberg.

[5] Semaev, I.A., 2004. Summation polynomials and the discrete logarithm problem on elliptic curves. IACR Cryptology ePrint Archive, 2004, p.31.

[6] Diem, C., 2013. On the discrete logarithm problem in elliptic curves II. Algebra and Number Theory, 7(6), pp.1281-1323.

[7] Gaudry, P., 2009. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. Journal of Symbolic Computation, 44(12), pp.1690-1702.

[8] Flynn, E.V., 1990, May. The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field. In Mathematical Proceedings of the Cambridge Philosophical Society (Vol. 107, No. 3, pp. 425-441). Cambridge University Press.

[9] Faugere, J.C., 1999. A new efficient algorithm for computing Gröbner bases (F4). Journal of pure and applied algebra, 139(1-3), pp.61-88.

[10] Bosma, W. and Cannon, J., 1993. MAGMA handbook. University of Sydney.

[11] Faugere, J.C., Horan, K., Kahrobaei, D., Kaplan, M., Kashefi, E. and Perret, L., 2017. Fast quantum algorithm for solving multivariate quadratic equations. arXiv preprint arXiv:1712.07211.

[12] Al-Daoud, E., 2007. Quantum Computing for Solving a System of Nonlinear Equations over GF (q). Int. Arab J. Inf. Technol., 4(3), pp.201-205.

[13] Harrow, A.W., Hassidim, A. and Lloyd, S., 2009. Quantum algorithm for linear systems of equations. Physical review letters, 103(15), p.150502.

[14] Shor, P.W., 1999. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), pp.303-332.

[15] Shafarevich, I.R. and Reid, M., 1994. Basic algebraic geometry (Vol. 2). Berlin: Springer-Verlag.

[16] Ding, J., Gower, J.E. and Schmidt, D., 2006. Zhuang-Zi: A New Algorithm for Solving Multivariate Polynomial Equations over a Finite Field. IACR Cryptology ePrint Archive, 2006, p.38.