MODIFIED BABY STEP GIANT STEP ALGORITHM TO SOLVE ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM (ECDLP)

A. Uma Maheswari[1], Prabha Durairaj[2]

[1]Associate Professor, Department of Mathematics, Quaid-E-Millath Government College for Women (Autonomous) Chennai - 600 002, India
[2]Head, Assistant Professor, Department of Mathematics, Quaid-E-Millath Government College for Women (Autonomous), Chennai - 600 002, India

---***---

Abstract - *A Modified version of Shanks' Baby-step Giant-step Algorithm to solve the Elliptic Curve Discrete Logarithm Problem is presented in this work. The algorithm is illustrated with numerical examples. The proposed algorithm is found to be more efficient than the existing algorithm in terms of computational complexity.*

Keywords: Elliptic curve groups, Discrete logarithm, Baby-step Giant-step algorithm.

AMS Subject Classification: 11Z05, 11T71.

1.Introduction

The discrete logarithm computation in finite groups is of considerable importance in Public Key Cryptography. The security of many Cryptographic schemes [1,2,3,4,5] depend on the apparent intractability of solving the discrete logarithm problem. The elliptic curve discrete logarithm problem (ECDLP) can be stated as follows: Given an elliptic curve E defined over a finite field F_q, a point $P \in E(F_q)$ of order N and a point $Q \in \langle P \rangle$, the subgroup generated by P, to find an integer k, $0 \le k \le (N-1)$ such that $Q = kP$. The integer k is called the discrete logarithm of Q to the base P denoted as $k = \log_P Q$.

Shanks' Baby-step Giant-step algorithm [6], the Pollard Rho algorithm [7] and the Pohlig-Hellman algorithm[8] are some of the well known generic algorithms to find discrete log while the Index Calculus algorithm [9] is a powerful non-generic algorithm. Shanks' algorithm computes discrete logarithms in a cyclic group G of order N in deterministic time $O(\sqrt{N})$ group operations and requires $O(\sqrt{N})$ group elements storage. Some variants of the Baby-step Giant-step algorithm to reduce the average case running time are due to Pollard [10], Bernstein and Lange [11]. The negation map can be used to speed up the computation of the ECDLP using the Baby-step Giant-step algorithm [12].

Variants of the discrete logarithm problem like the computation of discrete logarithms in small intervals [13] and the multidimensional DLP use the BSGS algorithm.

The computation of discrete logarithms in intervals is used in many public-key cryptographic protocols [14,15] and the multidimensional DLP is used in point counting algorithms [16].

In this work, a modified version of Shanks' algorithm to compute discrete logarithms in elliptic curve groups is presented. This algorithm is the elliptic curve analog of the new modified version of Shanks' algorithm devised by the authors[17].

The proposed algorithm factors the group order N into a product of two integers. This decomposition greatly reduces the number of giant-steps of the algorithm.

2.PRELIMINARY CONCEPTS

This section reviews the classical Baby-step Giant-step algorithm to find discrete logarithms in elliptic curve groups.

2.1. Shanks' Baby-step Giant-step algorithm

This is the first generic deterministic algorithm to find discrete log in arbitrary groups. The algorithm is based on the following observation.

Lemma[18]: Let n be a positive integer. If $r \in R, 0 \le r \le 1$ is given and if $m = \lceil n^r \rceil$, then there exist integers i and j such that $n = im + j$, $0 \le i < \left\lceil \frac{n}{m} \right\rceil$, $0 \le j \le (m-1)$.

We use the notation of the ECDLP as defined in the introduction. Given P and Q to find k such that $Q = kP, \quad 0 \le k < N$.

The algorithm is as follows[19]:

1. Fix $m = \lceil \sqrt{N} \rceil$ and compute mP
2. Compute the baby steps iP and store the pairs (iP, i) (sorted on the first component)
3. Compute the giant-steps $Q - jmP$ for $j = 0,1,2,\ldots(m-1)$ until where is a match with an element in the stored list.
4. When a match $iP = Q - imP$ is found then $k = i + jm (\mathrm{mod}\, N)$

The algorithm rans in approximately $\sqrt{N}$ time and requires $\sqrt{N}$ space.

3.THE NEW MODIFIED BABY-STEP GIANT-STEP ALGORITHM

In this section the new modified Baby-step Giant-step algorithm to find discrete logarithms in elliptic curve groups is presented. The algorithm is illustrated with numerical examples.

Given an elliptic curve E defined over a finite field F_q, a point $p \in E(F_q)$ of order N and a point $Q \in \langle P \rangle$, the subgroup generated by P, to find an integer k, $0 \le k \le (N-1)$ such that $Q = kP$

The following lemma which forms a basis for the new modified algorithm is proved.

Lemma 3.1: Let $E(F_q)$ be an elliptic curve group and $P \in E(F_q)$ be a point of order N. (If N is prime, choose any composite integer $n \ge N$ and let $n = uv$, $u > v$). Let $l = \lceil u \rceil$, $m = \lceil v \rceil$. Then given any point $Q \in \langle P \rangle$, the subgroup generated by P, there exist some pair of integers i, j, $0 \le i \le (m^2 - 1)$, $0 \le j \le (l^2 - 1)$ such that $Q = kP$ where $k = l^2 i + j$.

Proof: Let L_1 be the list $\{jP\}$, $j = 0$ to $(l^2 - 1)$. (baby steps) corresponding to the point Q, let L_2 be the list $\{Q - il^2 P\}$, $i = 0$ to $(m^2 - 1)$ (giant steps). Then there exist at least one collision in L_1 and L_2. (i.e) one pair $(jP, Q - il^2 P)$ such that $jP = Q - il^2 P$ or $Q = (l^2 i + j)P$.

The following discussion shows that such a collision certainly exists.

If $k = \log_P Q$, since $Q \in \langle P \rangle$, we have $0 \le k \le (N-1) \le (n-1) \le (l^2 m^2 - 1)$ where $k = \log_P Q$. Let $k_0 \equiv k (\mathrm{mod}\, l^2)$ so that $0 \le k_0 < l^2$. Let $k_1 = \frac{(k - k_0)}{l^2}$ then $k = k_0 + k_1 l^2$. We claim that $k_1 \le (m^2 - 1)$ because $k_1 = \frac{1}{l^2}(k - k_0) < \frac{k}{l^2} < \frac{l^2 m^2}{l^2} < m^2$.

We try all the i in the range $0,1,\ldots(m^2 - 1)$ and all the j in the range, $j = 0,1,\ldots(l^2 - 1)$, to find i, j such that $jP = Q - il^2 P$; In fact for $i = k_1$ and $j = k_0$, we have $Q - k_1 l^2 P = kP - k_1 l^2 P = (k - k_1 l^2)P = k_0 P$ so there is a match.

The proposed Modified Baby-step Giant-step algorithm is presented.

Algorithm 3.2:

Input: The order N of the cyclic subgroup, the generator P and the point Q.

Output: A value k such that $Q = kP$.

1. Choose any composite integer $n \ge N$
2. Factor n as the product of 2 integers u and v where $u > v$. So that $n = uv$. (The optimal choice of u and v would be that which minimizes the number of giant-step without drastically increasing the baby steps)
3. Set $l = \lceil \sqrt{u} \rceil$, $m = \left| \sqrt{v} \right|$ and compute $l^2 P$
4. For $j = 0$ to $(l^2 - 1)$ compute and store the pair (j, jP) and sort the list in some consistent way.
5.For $i = 0$ to $(m^2 - 1)$ compute $Q - il^2 P$ until there is a match in the second co-ordinate of an element in the stored list.
6. When a match $jP = Q - il^2 P$ is found, then return $k \equiv l^2 i + j (\mathrm{mod} \quad N)$

Note: The point jP is calculated by adding P (a "baby step") to $(j-1)P$. The point $Q-il^2P$ is computed by adding $-l^2P$ (a "giant step") to $Q-(i-1)l^2P$.

Also, to save storage space, one could store only the x co-ordinates of the point jP (along with the corresponding integer j), since looking for a match with jP requires only the x co-ordinate (assuming that we are working with a Weierstrass equation). When a match is found the two possible y coordinates can be recomputed.

To speed up the above algorithm, we present a second modified version of the Baby-step Giant-step algorithm. The following lemma which forms a basis for this new second version of the algorithm is proved.

Lemma 3.3: Let k be an integer with $|k|< l^2m^2$. Then there exist integers k_0 and k_1 with $\frac{-l^2}{2}<k_0\le\frac{l^2}{2}$ and $-m^2\le k_1\le m^2$ such that $k=k_0+l^2k_1$

Proof: Let $k_0\equiv k \pmod{l^2}$ with $\frac{-l^2}{2}<k_0\le\frac{l^2}{2}$.

Let $k_1=\frac{(k-k_0)}{l^2}$ then $k=k_0+l^2k_1$.

Then
$$\begin{aligned}|k_1| &\le \frac{1}{l^2}(|k|+|k_0|),\\ &<\frac{1}{l^2}\left(l^2m^2+\frac{l^2}{2}\right)\\ &<\left(m^2+\frac{1}{2}\right)\\ &<(m^2+1)\end{aligned}$$

So steps (4) to (6) of algorithm 3.2 can be modified and the second modified version of the algorithm is as follows.

Algorithm 3.4:

Input: The order N of the cyclic subgroup, the generator P and the point Q.

Output: A value k such that $Q=kP$.

1. Choose any composite integer $n\ge N$
2. Factor n as the product of 2 integers u and v where $u>v$. So that $n=uv$. (The optimal choice of u and v would be that which minimizes the number of giant-step without drastically increasing the baby steps)
3. Set $l=\lceil\sqrt{u}\rceil, m=\lceil\sqrt{v}\rceil$ and compute l^2P
4. Compute and store a list of the x- co-ordinates of jP for $j=0,1,\ldots\frac{l^2}{2}$ (i.e) store $(j,x(jP))$
5. Compute the points $Q-il^2P$ for $i=0,1,\ldots(m^2-1)$ until the x- co-ordinate of one of them matches with an element from the stored list.
6. Check whether $Q-il^2P=jP$ or $-jP$
7. If $\pm jP=Q-il^2P$, we have $Q=kP$ with $k=l^2i+j(\bmod N)$.

We are assured of a match $\pm jP=Q-il^2P$ for that particular pair (i,j) with $i=k_1$ and $j=|k_0|$ (refer Lemma 3.3) because

$$\begin{aligned}Q-il^2P &= kP-il^2P\\ &=(k-k_1l^2)P\\ &=k_0P=\pm jP \text{ with } j=|k_0|\end{aligned}$$

The Algorithm 3.2 is illustrated with a numerical example.

Example 3.5: Let $G=E(F599)$ where is the elliptic curve given by $y^2=x^3+1$. Let $P=(60,19)$ and $Q=(277,239)$. If P has order $N=600$, find the discrete log of Q to the base P.

This problem is worked out using the new modified algorithm as follows.

$N=600=40\text{x}15=uv$ where $u=40, v=15$ $l=\lceil\sqrt{u}\rceil$ $=\lceil\sqrt{40}\rceil=7$, $l=\lceil\sqrt{v}\rceil$ $=\lceil\sqrt{15}\rceil=4$ performing the baby steps one obtains the list (j,jP), $j=0,1,\ldots(l^2-1)$ i.e. $j=0,1,\ldots48$.

J	jP	j	jP
1	1P= (60,19)	25	25P = (351, 183)
2	2P=(305, 527)	26	26P = (239, 193)
3	3P=(329, 543)	27	27P = (513, 143)
4	4P=(340, 53)	28	28P = (563, 400)
5	5P=(32,254)	29	29P = (231, 04)
6	6P=(77, 359)	30	30P = (577, 517)
7	7P=(263, 114)	31	31P = (42, 47)
8	8P=(40, 551)	32	32P = (529, 45)
9	9P=(344, 587)	33	33P = (34, 455)

10	10P=(199, 302)	34	34P = (570, 562)
11	11P=(562, 506)	35	35P = (502, 349)
12	12P=(97, 457)	36	36P = (49, 38)
13	13P=(492, 339)	37	37P = (92, 363)
14	14P=(4, 444)	38	38P = (1, 166)
15	15P=(87, 218)	39	39P = (527, 576)
16	16P=(24, 446)	40	40P = (147, 35)
17	17P = (279, 532)	41	41P = (182, 172)
18	18P = (455, 65)	42	42P = (159, 284)
19	19P = (62, 463)	43	43P = (273, 28)
20	20P = (44, 538)	44	44P = (165, 584)
21	21P = (520, 77)	45	45P = (115, 227)
22	22P = (409, 299)	46	46P = (149, 385)
23	23P = (68, 565)	47	47P = (442, 234)
24	24P = (75, 305)	48	48P = (205, 547)

Performing the Giant steps one obtains the list $(i, Q - il^2P)$ for $i = 0,1,\ldots(m^2-1)$ i.e. $i = 0,1,\ldots 15$.

i	Q- i(49P)	i	Q- i(49P)
0	(277; 239)	8	(588; 59)
1	(553; 473)	9	(175; 440)
2	(378; 110)	10	(23; 230)
3	(261; 8)	11	(154; 296)
4	(556; 373)	12	(18; 439)
5	(520; 77)	13	(515; 327)
6	(563; 199)	14	(443; 484)
7	(432; 568)	15	(83; 447)

There is a match in the second coordinates of the two lists when $i = 5$, $j = 21$. Hence the discrete log of Q to the base P is found as $k \equiv l^2 i + j(\bmod N) = 49*5+21 = 266$.

The new modified algorithm uses only 15 giant steps where as the Classical Shanks' algorithm would use atmost 25 $\left(\left|\sqrt{n}\right| = \lceil\sqrt{600}\rceil = 25\right)$ giant steps. Observing that the baby steps are a one-time computation and giant steps are a repetitive computation (different for different elements Q) we observe that the number of giant steps are greatly reduced in the new modified algorithm when discrete log of several group element are to be found.

CONCLUSION

A Modified Shanks' Baby-step Giant-step algorithm has been proposed in this work to compute discrete logarithms in elliptic curve groups. This new modified algorithm significantly reduces the number of giant steps performed by factoring the group order N. This modified algorithm finds its best use when discrete logarithms of several group elements are to be found.

References:

[1] Elgamal.T, "A Public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory IT-31, 1985, pp 469-472.

[2] Diffie.W and Hellman.M.E, "New directions in cryptography," IEEE Transactions on Information Theory, IT-22, 1976, pp 644-654.

[3] Massey.J.L, "Logarithms in finite cyclic groups - cryptographic issues," Proceedings of 4th Benelux Symposium on Information Theory, 1983, pp 17-25.

[4] "Digital Signature standard", Federal Information Processing Standard (FIPS) Publications, 186, 1994.

[5] Schnorr.C.P, "Efficient Identification and signatures for smart cards," Advances in Cryptology- Crypto' 89, volume 435 of Lecture Notes in Computer Science, pp 239-252, Springer-Verlag, 1990.

[6] Shanks.D, "Class number, a theory of factorization and genera," Proc. Symposium Pure Math.20, pp 415-440, AMS, Providence, R.I., 1971.

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

[8] Pohlig.S.C and Hellman.M, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, IEEE Transactions on Information Theory IT-24, 1978, pp 106-110.

[9] Adleman.L.M, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography," Proc. 20th IEEE Found. Computer Science Symposium, pp 55-60, 1979.

[10] Pollard. J, "Kangaroos, Monopoly and discrete logarithms,", Journal of Cryptology 13(2000), pp 437-447.

[11] Bernstein.D.J and Lange.T, "Two grumpy giants and a baby," Proceedings of the Tenth Algorithmic Number Theory Symposium, MSP, Vol.1, 2013, (eds) E.W.Howe and K.S.Kedlaya, pp 87-111.

[12] Steven D.Galbraith, Ping Wang and Fangguo Zhang, "Computing elliptic curve discrete logarithms with improved baby-step giant-step algorithm", American Institute of Mathematical Sciences, 11(3), (2017), 453-469.

[13] Galbraith.S.D, Pollard.J.M and Ruprai.R.S, "Computing discrete logarithms in an interval,", Math. Comp., 82, No.282, 2013, pp 1181-1195.

[14] Boneh.D, Goh.E and Nissim.K, "Evaluating 2-DNF formulas on ciphertexts" in J.Kilian (ed.), Theory of Cryptography - TCC 2005, Springer LNCS 3378 (2005), pp 325-341.

[15] Henry. R, Henry.K and Goldberg.I, "Making a nymbler Nymble using VERBS," in M.J. Atallah and N.J.Hopper (eds), PETS 2010, Springer LNCS 6205 (2010) 111-129.

[16] Gaudry.P and Schost.E, "A low-memory parellel version of Matsuo, Chao and Tsujii's algorithm," in D.A.Buell (e.d), ANTS VI, Springer LNCS 3076(2004), 208-222.

[17] Uma Maheswari. A and Prabha Durai raj, Modified Shanks' Baby-step Giant-step algorithm and Pohlig Hellman Algorithm, International Journal of Pure and Applied Mathematics, Vol.118, No.10, (2018), pp 47-56.

[18] Odlyzko.A.M, "Discrete Logarithms in finite fields and their cryptographic significance," Advances in Cryptology, Proceedings Eurocrypt 84, Springer, 1985, pp 224-314.

19] Lawrence. C .Washington, Elliptic Curve, Number Theory and Cryptography, Second Edition, Taylor and Francis group, (2008) pp 146.