IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

A Review: Solving ECDLP Problem using Pollard's Rho Algorithm

Santosh P. Lokhande[1], Dr. Indivar Gupta[2], Dr. Dinesh B. Kulkarni[3]

Student, M.Tech, Computer Science and Engineering (Specialization in Information Technology) Walchand College of Engineering, Sangli, Maharashtra, India[1]

Scientist, Scientific Analysis Group (SAG), Defence Research and Development Organization, New Delhi, Delhi[2]

Professor, Department of Information Technology Walchand College of Engineering, Sangli, Maharashtra, India[3]

Abstract: In Public Key Cryptography system, separate keys are used to encode and decode the data. Public key being distributed publicly, the strength of security depends on large key size. The discrete logarithm for mathematical base in Public Key Cryptography systems. Unlike the finite field Discrete Logarithm Problem; there are no general purpose sub exponential algorithms to solve the Elliptic Curve Discrete Logarithm Problem. Though good algorithms are known for certain specific types of elliptic curves, all known algorithms that apply to general curves take fully exponential time. As a result, elliptic curves are gaining popularity for building cryptosystems. The absence of sub exponential algorithms implies that smaller fields can be chosen compared to those needed for cryptosystems. Elliptic curve based cryptosystems are popular because they provide good security at key sizes much smaller than number theoretical Public Key Schemes like RSA cryptosystem. Solving Elliptic Curve Discrete Logarithm Problem using Pollard's Rho algorithm provide efficiency in terms of time and storage. Using various parallel architectures like MPI, GP-GPU and FPGA increase accessing precision and efficiency of solving ECDLP.This article covers Elliptic Curve Cryptography, Elliptic Curve Discrete Logarithm Problem and Pollard's Rho algorithms to solve ECDLP.

Keywords: Elliptic curve, ECC, DLP, ECDLP, Pollard's Rho Algorithm, Parallel Architectures.

I. INTRODUCTION

The first practical realization followed in 1977 when Ron Rivest, Adi Shamir and Len Adleman proposed their now well-known RSA cryptosystem, in which security is based on the intractability of the integer factorization problem. Elliptic curve cryptography (ECC) was discovered in 1985 by Neal Koblitz and Victor Miller [2]. Elliptic curve cryptographic schemes are public-key mechanisms that provide the same functionality as RSA schemes. However, their security is based on the hardness of Elliptic Curve Discrete Logarithm Problem (ECDLP). For example, it is generally accepted that a 160-bit elliptic curve key provides the same level of security as a 1024-bit RSA key [3]. The advantages that can be gained from smaller key sizes include speed and efficient use of power, bandwidth, and storage. Due to smaller key size, implementation of elliptic curve based cryptosystems requires less memory. Therefore elliptic curve based cryptosystems have become popular in small devices such as Smart cards, PDA providing good amount of security.

The strength of elliptic curve cryptosystem is directly proportional to the order of the underlying finite field. As the field order increases the hardness of the cryptography system increases. Traditional methods are not capable to solve the ECDLP in polynomial amount of time. Pollards Rho Algorithm, proposed by J.M Pollard [4], gives good results in terms of time and space to solve ECDLP problem. The growing parallel architectures enable us to make the use of parallelized versions of algorithm for time optimization.
The paper is organized as follows. The second section covers the related work done in solving the ECDLP problem. Third section covers the background of elliptic curve cryptography, Discrete Logarithm Problem (DLP), ECDLP problem. Fourth section covers Pollard's Rho algorithm. Fifth section covers parallel version of Pollard's Rho algorithm.

II. RELATED WORK

To check the strength of cryptographic systems a lot of attacks have been attempted on the systems. Large amount of work has been carried out in solving the integer factorization problem (IFP), discrete logarithm problem in multiplicative group of finite field (DLP) and in the group points on an elliptic curve (ECDLP). The concept of elliptic curve cryptography was put forward by V. Miller in 1986 [2], after that N. Koblitz, A. Menezes and S. Vanstone in

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

2000 [4], in these papers they proposed a system which uses the elliptic group E (Fq), defined over a finite field Fq as an arithmetic base of cryptosystem.
The most particularly used method for solving the ECDLP was Pollard's Rho method. Number theorist J. M. Pollard's has introduced the pollard's algorithm in 1978 [4]. After that a lot of work has been carried out to solve the problem of DLP. The ECDLP also got the solution through the use of a Pollards rho algorithm.

III.BACKGROUND

A. Elliptic Curves Cryptography:
Let K be a finite field, set E of points (x, y) satisfying the equation $y^2 = x^3 + ax + b$ with a, b ∈ K, is called elliptic curve whenever x^3+ax+b has no multiple roots in K. The definition of an elliptic curve is slightly more complicated in when the characteristic of K is 2 or 3. If K = R, the real field, then the addition can be described geometrically through the method "chord-tangent".The inverse of a point P = (x, y) is −P = (x, −y) by definition. Moreover, following explicit formulas are for the sum and the doubling of points on E(R). If P =(x_1, y_1), Q = (x_2, y_2) and P + Q = (x_3, y_3),

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

And λ is slope of the line passing through point P and Q .

If P≠Q

$$\lambda = \frac{(y_2 - y_1)}{(x_2 - x_1)}$$

If P = Q, that is point doubling of point P then

$$\lambda = \frac{(3{x_1}^2 + a)}{2y1}$$

Indeed, V. Miller [2] and N. Koblitz [4] proposed (independently each other) to use the elliptic group E(Fp), defined on a finite field Fp, as an arithmetic base of a cryptosystem.

B. Elliptic Curve Discrete Logarithm Problem:
Discrete logarithms [5] [12]are thus the finite group-theoretic analogue of ordinarylogarithms, which solve the same equation for real numbers b and g, where b is the base of the logarithm and g is the value whose logarithm is being taken. In the same way elliptic curve discrete logarithm problem can be formulated as it follows:given P, Q ∈ E(K), determine the integer k so that

$$Q = kP = P + P + \ldots + P \text{(k times P)}$$

This problem is significantly hard if the ground field is finite. Although ECDLP is a particular case of DLP, there is no generic algorithm with sub exponential running time that solves it. Since all special attacks to the ECDLP can be easily avoided by means of a suitable choice of the parameters, it is more interesting to focus on generic algorithms.The most used generic method is Pollard's rho method.

IV. POLLARD'S RHO ALGORITHM

The Pollard's Rho algorithm was first proposed by mathematician J. M. Pollard in 1978 [4]. The general Pollard's rho algorithm was designed to work for the DLP problem; after it has been designed for solving ECDLP problem. Let P and Q be two points on elliptic curve E, and Q be in the cyclic subgroup generated by P, Q∈<P>. Let n be the order of the generator point P. We have to find the positive integer k such that Q= kP. Iteration function defines the random cyclic walk of points over the subgroup. An iteration function is that they update a state of triplet (c, d, X).
The main idea behind Pollard's rho algorithm is to find distinct pairs (c',d') and(c",d") of integers modulo n such that

$$c'P + d'Q = c"P + d"Q$$

Then

$$(c' - c")P = (d" - d')Q = (d" - d')kP$$

And so

$$(c' - c") = (d" - d')k(\mathrm{mod} n)$$

Hence $k = \log_P Q$ can be obtained by computing

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

$$k = (c' - c'')(d' - d'')^{-1}(\mathrm{mod} n)$$

Use of Floyd's detection algorithm reduces the storage requirement, keeping the time requirement unchanged. The above algorithm has been devised in such a way that it will require negligible amount of memory. At any instance only the current values of X'_i and X''_i will be in memory for comparison. But the total computation has been increased, due to which it is not possible to solve large ECDLP problems.

V. PARALLEL POLLARD'S RHO ALGORITHM

The idea of parallel Pollard's rho algorithm was first put forward by Van Orschot and Wiener [10] in 1999. The idea yields a factor M speedup when M processors are employed. The idea is to allow the sequences $\{X_i\}_{i>=0}$ to collide with one another necessarily generated by different processors. More precisely, each processor randomly selects its own starting point X_0, but all use the same iteration function f to compute subsequent points X_{i+1}. Thus, if the sequences generated from two different processors ever collide then two sequences will be identical from that point on.

A. GPU Based Implementation of Pollard's Rho Algorithm:
The idea of using cuda technology for implementation of Pollard's Rho is forward by M. Chinnicia [8] and S.B. Khemnar [7]. The implementation is summarized as follows:
1. The host makes pre-computations needed for the Pollard's rho algorithm. Precomputed data is sent to the compute device (GP-GPU).
2. The GP-GPU threads generate pseudorandom points through the iteration function, which looks for distinguished points and report to the host.
3. The distinguished points are stored into a hash table, where the host looks for collisions. The algorithm stops if a collision is found.

In M. Chinnicia [8] consideration most delicate part is modular multiplication via Montgomery product. The starting points are linear combinations of P and Q. Each point is generated with different multiple of P. If t threads are executed, each of them are associated with starting point. The iteration function is called add only function which partitions <P> into r subsets. Each thread iterates through points in the cyclic subgroup and sends only those points to root that satisfy the group property.
The GP-GPU technology supports arithmetic operation for 32-bit numbers only. ECDLP problem for 32-bit prime field only in [7]. For solving ECDLP problem for big Integers, an arithmetic library needed which can help to perform operation on large integers.

B. MPI Based Implementation of Pollard's Rho Algorithm:
The idea of using MPI technology for implementation of Pollard's Rho is forward by K.A. Chavan [9]. As the arithmetic operations in the group of elliptic curve require more computational cost, specialized libraries can be used to perform those operations. GMP, GP- PARI, rosing, miracl etc. are some of the examples of such libraries. PARI/GP [11] is a widely used computer algebra system designed for fast computation in number theory (factorization, algebraic number theory, elliptic curves, etc.). PARI/GP is also available as a C library to allow faster computation.
MPI technology has been used to parallelize the algorithm. MPI technology allows to run the program on cluster of machine. MPI technology provides a sophisticated way of communication between these machines. The idea yields a factor M speedup when M processors are employed. More precisely, each processor randomly selects its own starting point X_0, but all use the same iteration function f to compute subsequent points X_{i+1}. Thus, if the sequences generated from two different processors (processes) ever collide, then, two sequences will be identical from that point on. Iteration function which is responsible for a pseudo random walk in group is the important part of Pollard's Rho Algorithm.
ECDLP problem for finite prime field of 85-bit using MPI technology was solved in [9] with help of PARI/GP library.

VI. CONCLUSION AND FUTURE WORK

Despite the several decades' long history of the elliptic curve cryptography, there is still a lack of research. It is possible to conclude that the lack of research is related to the relatively complex mathematical foundation of elliptic curves and lack of interest from the systems developers. As mentioned, the discrete logarithm problem is algorithmically harder than the integer factorization problem, allowing a significant reduction in the public key cryptographic key size, thus speeding up a variety of cryptographic operations. Elliptic curve based cryptosystems can be effectively used on low resources and power system solutions such as smart cards, mobile devices, sensors and so on.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

The future of ECC looks brighter than RSA as today's applications (smart cards, pagers, and cellular telephones etc.) cannot afford the overheads introduced by RSA. At least, in today's small computing devices ECC can be used for encryption and decryption as it requires smaller key sizes and has lesser computing complexity as compared to RSA. Solving ECDLP problem using parallel version of pollard's rho algorithm makes the efficient use of available resources and can give a speedup of M when M processors are employed. Existing solution using GP-GPU [7] [8] to solve ECDLP is not sufficient. Because GP-GPU doesn't support big Integers. So use a big Integer library will help to solve ECDLP on GP-GPU for prime field greater than 32-bit. Checking the time and space complexity of the algorithm when implemented on HPC cluster using GP-GPU with help of Big Integer library is of great interest.

ACKNOWLEDGMENT

We sincerely thank all the authors, whose papers are in the area of Elliptic Curve Cryptography. Also, we would like to thank, Dr. Indivar Gupta (Scientist 'E' at DRDO, New Delhi) who permitted to work at their premise and provided insight and expertise that greatly assisted the research.

REFERENCES

[1] D. Hankerson, S. Vanstone, and A. J. Menezes, "Guide to elliptic curve cryptography". 2004.
[2] V. Miller, "Use of Elliptic Curves in Cryptography," Adv. Cryptol. – CRYPTO'85, vol. LNCS 218, pp. 417–426, 1986.
[3] Soram Ranbir Singh,Ajoy Kumar Khan and Soram Rakesh Singh, "Performance Evaluation of RSA and Elliptic Curve cryptography". 2016
[4] N. Koblitz, A. Menezes, and S. Vanstone, "The State of Elliptic Curve Cryptography," Des. Codes Cryptogr., vol. 193, no. 2, pp. 173–193, 2000.
[5] Kevin S. McCurely, " The Discrete Logarithm Problem", vol. 42 , pp. 49-74. 1990
[6] J. M. Pollard, "Monte Carlo methods for index computation," Mathematics of Computation, vol. 32, no. 143. pp. 918–924, 1978.
[7] S. B. Khemnar, R. Chaudhary, and D. B. Kulkarni, "CUDA based Implementation of Parallelized Pollards Rho Algorithm for ECDLP : A Review", Data Mining and Knowledge Engineering," vol. 70, no. 234, pp. 2–3, 2016.
[8] M. Chinnicia, S. Cuomo, M. Laporta, and V. Cinthia, "CUDA based implementation of parallelized Pollard's Rho algorithm for," pp. 1–5, 2006.
[9] K. A. Chavan, I. Gupta, and D. B. Kulkarni, "A Review on Solving ECDLP over Large Finite Field Using P arallel Pollard ' s Rho (ρ) Method," vol. 18, no. 2, pp. 1–11, 2016.
[10] P. C. van Oorshant and M. J. Wiener, "Parallel Collision Search with Cryptanalytic Applications", Journal of Cryptology, volume 12 No. 1, pages 1-28, 1999.
[11] http://pari.math.u-bordeaux.fr/
[12] https://en.wikipedia.org/wiki/Discrete_logarithm

BIOGRAPHIES

Santosh P. Lokhande is currently pursuing M.Tech. Degree in Computer Science and Engineering (Specialization in Information Technology) Walchand College of Engineering, Sangli, Maharashtra, India 416415. His research area includes High performance computing, Cloud Computing, Information Security.

Dr. Indivar Gupta is Scientist in Scientific Analysis Group, DRDO, New Delhi, India. His research area includes High Performance Computing, Number Theory, and Information Security.

Dr. Dinesh B. Kulkarni is Professor in Department of Information Technology Walchand College of Engineering, Sangli, Maharashtra, India 416415. His research area includes Parallel Programming, Image coding, High Performance computing, Computer Network, Machine learning.