Pollard Rho Algoritm For Elliptic Curve Cryptography

Deepthi P,
Assistant Professor,
Computer Science & Engineering Department,
Bhoj Reddy Engineering College for Women,
Vinay nagar, Santhonagar, Saidabad,
Hyderabad-500059, India.

Abstract*—Digitization has transformed our world. The way we live, work, play, and learn have all changed. Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. "Network security" is the security provided to a network from unauthorized access and risks. It refers to any activity designed to protect the usability and integrity of network and data that includes both hardware and software technologies. Elliptic curve cryptography (ECC) is one of the most powerful type of cryptographic technic widely in use today.*

***Keywords*— Cryptography, Security, Elliptic curve, Elliptic curve cryptography, Discrete logarithm problem, pollard rho.**

I.INTRODUCTION

Public key cryptography or **asymmetric cryptography**, is any cryptographic system that uses pairs of keys: *public keys* which may be disseminated widely and *private keys* which are known only to the owner. This accomplishes two functions: authentication, which is when the public key is used to verify that a sender of the paired private key sent the message, and encryption, whereby only the receiver of the paired private key can decrypt the message encrypted with the public key.

In a public key encryption system, any person can encrypt a message using the public key of the receiver, but such a message can be decrypted only with the receiver's private key. For this to work it must be computationally easy for a user to generate a public and private key-pair to be used for encryption and decryption. The strength of a public key cryptography system relies on the degree of difficulty (computational impracticality) for a properly generated private key to be determined from its corresponding public key. Security then depends only on keeping the private key private, and the public key may be published without compromising security.

II.Ellipticcurve

Ellipticcurves are believed to providegood security withsmallerkey sizes,somethingthatis very usefulin many applications. An elliptic curve is a curve that's also naturally a group. The group law is constructed geometrically. Elliptic curves appear in many diverse areas of mathematics, ranging from number theory to complex analysis, and from cryptography to mathematical physics.An elliptic curve is the set of points that satisfy a specific mathematical equation.

The equation for an elliptic curve is:

$$y^2 = x^3 + ax + b$$

That graphs like this:

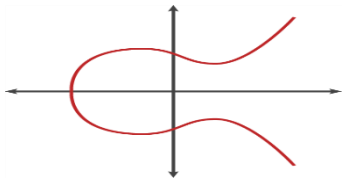

Figure1: Elliptic Curve

There are other representations of elliptic curves, but technically an elliptic curve is the set of points

satisfying an equation in two variables with degree two in one of the variables and three in the other. An elliptic curve is not just a pretty picture, it also has some properties that make it a good setting for cryptography.

III. Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography.Elliptical curve cryptography (ECC) is a public keyencryption technique based on *elliptic curve theory* that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman
Elliptic curve cryptography (ECC) is increasingly used in practice to instantiatepublic-key cryptography protocols, for example implementing digital signatures and key agreement. With ECC, you can use smaller keys to get the same level of security. The key size should be small because more and more cryptography is done on less powerful devices like mobile phones. The biggest differentiator between ECC and RSA is key size compared to cryptographic strength.

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

In the table above, ECC is able to provide the same cryptographic strength as an RSA-based system with much smaller key sizes. For example, a 256 bit ECC key is equivalent to RSA 3072 bit keys.

IV. Elliptic Curve Discrete Logarithm

The elliptic curve discrete logarithm problem is the cornerstone of much of present-day elliptic curve cryptography. It relies on the natural group law on a non-singular elliptic curve which allows one to add points on the curve together. Given an elliptic curve E over a finite field F, a point on that curve, P, and another point you know to be an integer multiple of that point, Q, the "problem" is to find the integer n such that nP=Q.

The problem is computationally difficult unless the curve has a "bad" number of points over the given field, where the term "bad" encompasses various collections of numbers of points which make the elliptic curve discrete logarithm problem breakable. For example, if the number of points on E over F is the same as the number of elements of F, then the curve is vulnerable to attack.

V. Pollard Rho

In 1978, Pollard came up with a "Monte-Carlo" method for solving the discrete logarithm problem. Since then the method has been modified to solvethe elliptic curve analog of the discrete logarithm problem. As the Pollard-Rhoalgorithm is currently the quickest algorithm to solve the Elliptic Curve DiscreteLogarithm, so the security of the elliptic curve cryptosystem depends on theefficiency of this algorithm. Theoretically, if the Pollard-Rho algorithm is able tosolve the ECDLP efficiently and in a relatively short time, then the system will berendered insecure.The strategy of the algorithm is to produce a sequence of randomly generatedterms (Ri,ai,bi), whereRiis a point on the the curveEandai,bilie inFp,overwhich the elliptic curveEis defined. SinceE(Fp) is a finite group, the sequence eventually becomes periodic and loops back to an earlier term in the sequence. We use this periodicity to solve the ECDLP. Since the sequence does not always loopback to the first term, a diagram of the sequence looks like the Greek letterρ(Seefigure 2). That is why this method is called the Pollard-Rhomethod.

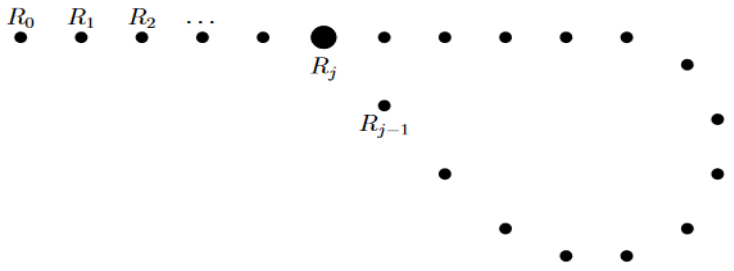

Figure 2: Diagram of the sequence produced by the Pollard Rho algorithm

VI. Pollard-Rho Method for Solving ECDLP

LetG=E(Fp), such that|G|=n,andPandQsuch thatQ=xPinG.Ouraim is to calculatex.

Pollard-Rho Algorithm

1. Using a hash function, we partitionGinto 3 sets,S1,S2,S3of roughly thesame size, butO/∈S2

2. Define an iterating functionfof a random walk:

$$R_{i+1} = f(R_i) = \begin{cases} Q + R_i, & R_i \in S_1; \\ 2R_i, & R_i \in S_2; \\ P + R_i, & R_i \in S_3 \end{cases}.$$

3. LetRi=aiP+biQ, and therefore

$$a_{i+1} = \begin{cases} a_i, & R_i \in S_1; \\ 2a_i \ mod \ n, & R_i \in S_2; \\ a_i + 1, & R_i \in S_3 \end{cases}$$

And

$$b_{i+1} = \begin{cases} b_i + 1, & R_i \in S_1; \\ 2b_i \ mod \ n, & R_i \in S_2; \\ b_i, & R_i \in S_3 \end{cases}$$

4. Start withR0=P, a0=1,b0=0and generate pairs(Ri,R2i)until a matchis found,

i.e.Rm=R2m

for somem.

Once we've found a match, we have

Rm=amP+bmQ

R2m=a2mP+b2mQ.

Hence we computexto be:

$$x = \frac{a_{2m} - a_m}{b_m - b_{2m}} \ (mod \ n).$$

VII. CONCLUSION

Many symmetric and asymmetric algorithms can be used for encryption, decryption, key exchange and digital signature. To break the prime factors of RSA algorithm we can use pollard rho integer factorization algorithm. As we have moved from RSA to elliptic curve cryptography because of its small key sizes we are trying to use pollard rho algorithm for discrete logarithms, which can be used to break the points on the elliptic curve.

In future a pollard rho algorithm can be modified to break elliptic curve cryptography.

VIII. REFERENCES

1. http://www.cisco.com/c/en/us/products/security
2. http://wstein.org/simuw06
3. https://www.math.brown.edu/~jhs/Presentations
4. http://homepages.warwick.ac.uk/~masiao/maths
5. https://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc
6. http://wstein.org/edu/2007/spring/ent
7. http://planetmath.org/ellipticcurvediscretelogarithmproblem