ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Elliptic Curve Cryptography-A new approach to Public Key Cryptography

Ajit Karki
MTech. (Computer Science and Engineering), Assistant Professor, Deptt. Of Computer Science, The ICFAI University, Sikkim, India
ajitkarki4@gmail.com

Abstracts

Elliptic curve cryptography (ECC) is an approach to public key Cryptography based on the algebraic structure of Elliptic curves over finite field. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography. An elliptic curve in cryptography was suggested independently by Neal Koblitz and Victor S. Millar in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005.Cryptography comes from Greek words meaning "hidden writing". Cryptography converts readable data or clear text into encoded data called cipher text. By definition cryptography is the science of hiding information so that unauthorized users cannot read it. It involves Encryption and decryption of messages. Encryption is the process of converting a Plain text into cipher text and decryption is the process of getting back the original Message from the encrypted text. ECC is a newer approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields, and considered a s a marvelous technique with low key size for the use r, and hard exponential time challenge for an intruder to break into the system. In ECC a 16 0 bits key, provides the same security as RSA [1] 1024 bits key, thus lower computation f aster cryptographic power is required. The advantage of elliptic curve cryptosystems is the absence of sub exponential time algorithms, for attack. As ECC uses less key size to provide more security, and for this advantage it is used to perform operations, running on smaller chips or m ore compact software. The public key cryptography- based r emote authentication schemes are not suitable for mobile devices, because of the limitation in the bandwidth, computational strength, power availability or storage in mobile devices. Elliptic Curve cryptography is very difficult to understand by attacker because it relies on Elliptic Curve Discrete Logarithm Problem known as ECDLP. So it is difficult to break.

Keywords: Elliptic Curve, cryptography, cryptosystem, RSA.

Introduction

Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible — this is the "elliptic curve discrete logarithm problem" or ECDLP. The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the difficulty of the problem. Consider the equation:**Q=kP,** where Q,P belongs to a curve (ECDLP).

Given k, P → "easy" to compute Q.
Given Q, P → "hard" to find k .

Elliptic curve cryptography was introduced in 1985 independently by Koblitz and Miller [1] as a promising alternative for cryptographic protocols based on the discrete logarithm problem in the multiplicative group of a finite field (e.g., Diffie-Hellman key Exchange [2] or ElGamal encryption/signature [1]).ECC is a kind of public key cryptosystem like RSA. But it differs from RSA in its quicker evolving capacity and by providing attractive and alternative way to researchers of cryptographic algorithm. The security level which is given by RSA can be provided even by smaller keys of ECC. For example, the 1024 bit security strength of a RSA could be offered by 163 bit security strength of ECC. Elliptical curve cryptography (ECC) is a public key encryption 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. Because ECC helps to establish equivalent security with

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

lower computing power and battery resource usage, it is becoming widely used for portable devices. An elliptic curve is not an ellipse (oval shape), but is represented as a looping line intersecting two axes (lines on a graph used to indicate the position of a point). ECC is based on properties of a particular type of equation created from the mathematical group (a set of values for which operations can be performed on any two members of the group to produce a third member) derived from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number was used, even if you know the original point and the result. Equations based on elliptic curves have a Characteristic that is very valuable for cryptography purposes: they are relatively easy to perform, and extremely difficult to reverse. For current cryptographic purposes, an elliptic curve is a plane curve which consists of the points satisfying the equation 1 along with a distinguished point at infinity (∞).

General form of an EC

- An elliptic curve is a plane curve defined by an equation of the form
  $y^2 = x^3 + ax + b$.

Example:

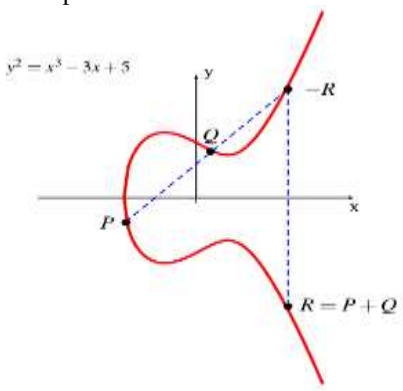

Figure 1: General form of an EC

Courtesy: V. Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology -CRYPTO'85, LNCS 218, pp.417-426.

Elliptical Curve Cryptography Background:

Public key cryptosystem gain more popularity since it was proposed by W. Diffie and M. Hellman in 1976, foundation of every cryptosystem is a hard mathematical problem that seems infeasible to solve. The techniques of the public key cryptosystems are classified into three categories,

1. Based on integer factorization problem, such as RSA [2]

2. Based on discrete log, such as Digital Signature Algorithm (DSA) [3].

3. Based on Elliptic curve, such as Elliptic curve Diffie Hellman (ECDH) [4].

Security degree of all the techniques depends on the hardness of mathematical problem. Elliptic curve is harder to solve, i.e. it takes full exponential time compare to other techniques. ElGamal proposes use of discrete log problem in asymmetric key cryptography in 1985. Elliptic curves are used in mathematics many years before but it can be used in the implementation of asymmetric key cryptography as suggested by Neal Koblitz and Miller independently in 1985. Elliptic curve group is defined over non- homogeneous (affine) weierstrass equation, Where a, b, c, d, e are real numbers. Elliptic curve cryptography is defined over special case of equation is Where 'a' and 'b' are real numbers. Necessary condition implement elliptic curve in cryptography, curve should be non-singular, condition for non-singular curve is $4a3+27b^2 \neq 0$. $4a3+27b^2$ *represents as Δ. All points (x, y) satisfying the equation* $y^2=x^3+ax+b$ *together point at infinity (O) lies on the elliptic curve. Elliptic curve group can be obtained by varying different 'a' and 'b' values.*

ECC Public Key Cryptosystem

In the public key elliptic curve cryptosystems, we assume that entity A wants to send a message m to entity B securely. Order of a point on the curve can be defined as a value n such that nP = P+P+..+P.. n times = O (infinity).

Key ***Generation***

Both the entities in the cryptosystem agree upon a, b, p, G, n which are called „Domain Parameters" of ECC. G is called generator point and n is the order of G. Now A generates a random number nA < n as his private Key and calculates his public key Set PA = G+G+G…+nA times. B generates a random number nB < n as his private Key and calculates his public key, set PB = G+G+G…+nB times..

Key Exchange

Entity A computes his Shared Key by Computing K = PA + PA +..+… nB times Entity A computes his Shared Key by Computing K = PB + PB +...+… nA times The two above keys have same value because: nA*PB = nA* (nB*G) = nB*(nA *G)= nB * PA2.4

Encryption

"A" selects a private key nA and generates a public key PA= nA *G.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

To encrypt and send a message 'Pm' to "B", "A" chooses a random positive integer 'k' and produces the cipher text '**C**m'consisting to the pair of points:
A sends Cm = 2 cipher text points those are:
{kG, Pm + k PB)}.
Where G - generator Point
Pm - plaintext point on the curve.
k - a random number chosen by A.
PB - public key of B.

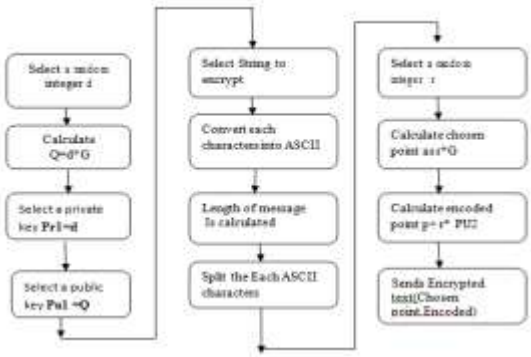

Figure: 2: Block Diagram of Encryption Process

Courtesy: N.Koblitz, "Uses of elliptic curves in cryptography" BBN Technologies, fourth edition.

Decryption

"B" multiplies the first point in the pair by B's Secret key and subtracts the result from the second point:

Pm + kPB - nB(kG) = Pm + k(nB)G - nB(kG) = Pm.

"A" has masked the message **P**m by adding k**P**B to it. Nobody but 'A' knows the value of 'k', so even though **P**B is a public key, nobody can remove the mask k**P**B.
For an attacker to recover the message, the attacker would have to compute k for given **G** and k**G**, which is hard.ECC Encryption and Decryption methods can only encrypt and decrypt a point on the curve not messages

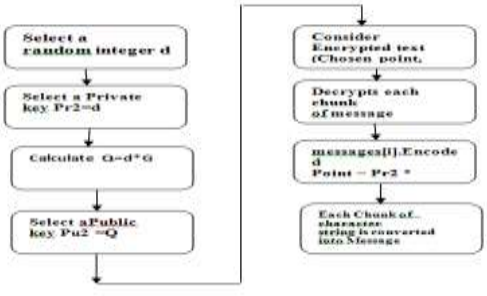

Figure: 2.1: Block Diagram of Decryption Process

Courtesy: Julio Lopez and Richard Dahab "Survey of Elliptic Curve Cryptography" ISSN: 0234-0512 & E-ISSN: 0244-0245, Volume 1, issue 1.

Encoding and decoding a message in the implementation of ECC

ECC Encryption and Decryption methods can only encrypt and decrypt a point on the curve not messages. Unfortunately, there are no known polynomial time algorithms for finding a large number of points on an arbitrary curve. We are not simply looking for random points on E, here. We want a systematic way of finding points on Ep(a,b) relating somehow to the plain text message. Therefore, we are forced to use probabilistic algorithms to do this, where the chance of failure is acceptably small. Thus Encoding (message to a point) and Decoding (point to a message) methods are important while Encryption and Decryption.

Message encoding and decoding

Let us suppose a text file has to be encrypted, a user can encrypt the ASCII code of each and every printable character on the keyboard , let us say he has to encrypt an 8-bit number , can represent 128 characters on the keyboard. Fig shows the sequence of steps to be followed when a message to be encrypted and decrypted using elliptic Curve Cryptography. All the points on the elliptic curve can be directly mapped to an ASCII value, select a curve on which we will get a minimum of 128 points, so that we fix each point on the curve to an ASCII value. For example, „ENCRYPT" can be written as sequence of ASCII characters that is „ 69" „78" „67" „82" „89" „80" „84" we can map these values to fixed points on the curve. This is easiest method for embedding a message but less efficient in terms of security. The steps to be followed during encoding and decoding.

Advantages and Disadvantages of ECC

ECC employs a relatively short encryption key - a value that must be fed into the encryption algorithm to decode an encrypted message. This short key is faster and requires less computing power than other first-generation encryption public key algorithms. For example, a 160-bit ECC encryption key provides the same security as a 1024-bit RSA encryption key and can be up to 15 times faster, depending on the platform on which it is implemented. RSA is a first-generation public-key cryptography technique invented by Ronald Rivest, Adi Shamir and Leonard Adleman in the late 70s. Both RSA and ECC are in widespread use. The advantages of ECC over RSA are particularly important in wireless devices, where computing power, memory

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

and battery life are limited. Summarizing the above discussions, following **advantages** can be derived:
• Size of the key: The size of the key required for encryption and digital signatures is surely far less than other systems.
• Less time for encryption.
• None of the currently known algorithms for the solution of the DL problem can be applied.
The use of brute force attack on ECC takes a lot longer time to be successful.
• Any cryptographic scheme/protocol based on discrete logarithms can be easily converted to elliptic curve form.

Disadvantages of using ECC:
• ECC utilizes elliptic curves, generators and finite fields, and points of a curve, which can lead to more complex calculations that could strain an embedded processor.
• This can be circumvented with lookup tables for elliptic curves, but this can eat up valuable resources on handheld and portable devices.
• ECC systems are slower than RSA in public key operations. So in applications requiring vast public key encryptions, the system is not desirable.

Elliptic curve cryptosystems strength

Majority of public key cryptosystems (RSA, DH) use either integer or polynomial arithmetic with very large numbers/polynomials. ECC imposes a significant load in storing and processing keys and messages. The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm problem. Let P and Q be two points on an elliptic curve such that kP=Q, where k is scalar. Given P and Q, it is computationally infeasible to obtain k, if k is sufficiently large. k is the discrete logarithm of Q to the base P.[6].

Elliptic curve security and efficiency

The majority of public key systems in use today use 1024-bit parameters for RSA and Diffie-Hellman. The US National Institute for Standards and Technology has recommended that these 1024-bit systems are sufficient for use until 2010. After that, NIST recommends that they be upgraded to something providing more security. The question is what should these systems be changed to? One option is to simply increase the public key parameter size to a level appropriate for another decade of use. Another option is to take advantage of the past 30 years of public key research and analysis and move from first generation public key algorithms and on to elliptic curves. One way judgments are made about the correct key size for a public key system is to look at the strength of the conventional (symmetric) encryption algorithms that the public key algorithm will be used to key or authenticate. Examples of these conventional algorithms are the Data Encryption Standard (DES) created in 1975 and the Advanced Encryption Standard (AES) now a new standard. The length of a key, in bits, for a conventional encryption algorithm is a common measure of security. To attack an algorithm with a k-bit key it will generally require roughly 2k-1 operations. Hence, to secure a public key system one would generally want to use parameters that require at least 2k-1 operations to attack. To use RSA or Diffie-Hellman to protect 128-bit AES keys one should use 3072-bit parameters: three times the size in use throughout the Internet today. The equivalent key size for elliptic curves is only 256 bits. One can see that as symmetric key sizes increase the required key sizes for RSA and Diffie-Hellman increase at a much faster rate than the required key sizes for elliptic curve cryptosystems. Hence, elliptic curve systems offer more security per bit increase in key size than either RSA or Diffie-Hellman public key systems. Security is not the only attractive feature of elliptic curve cryptography. Elliptic curve cryptosystems also are more computationally efficient than the first generation public key systems, RSA and Diffie-Hellman. Because of the key size ECC is more efficient public key cryptography. The main attraction of ECC over RSA is that ECC takes only 160 bit and provides the same security which can provide by RSA 1024 bits. it is suitable for low memory devices. Although elliptic urve arithmetic is slightly more complex per bit than either RSA or DH arithmetic, the added strength per bit more than makes up for any extra compute time.

Conclusion

Elliptic curve cryptography has been emerged as a vast field of interest for application specific security requirements. It has its roots into the number theory which was already used for cryptographic applications before ECC. The elliptic curve discrete logarithm problem makes ECC most efficient with smaller key size compared to earlier RSA algorithm. It is mostly considered for resource constrained devices. Research in the field of Elliptic Curve Cryptography has emerged in various directions to analyze its proper implementation on hardware as well as software platforms.

References

1. B.Schneier. Applied Cryptography. John Wiley and Sons, second edition, 2012.
2. Cryptography and Elliptic Curves, koblitz, second edition, 2011.
3. Julio Lopez and Ricardo Dahab, “An overview of elliptic curve cryptography”, May 2011.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

4. V. Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology - CRYPTO'85, LNCS 218, pp.417-426, 2011.
5. Jeffrey L. Vagle, "A Gentle Introduction to Elliptic Curve Cryptography", BBN Technologies, 2010
6. Mugino Saeki, "Elliptic curve cryptosystems", M.Sc. thesis, School of Computer Science, McGill University, 2010.
7. J. Borst, "Public key cryptosystems using elliptic curves", Feb. 2010.
8. Aleksandar Jurisic and Alfred Menezes, "Elliptic Curves and Cryptography", Dr. Dobb's Journal, April 2010.
9. Robert Milson, "Introduction to Public Key Cryptography, april 2009.
10. Aleksandar Jurisic and Alfred J. Menezes, Elliptic Curves and Cryptography, 2008.
11. V. S. Miller, "Use of Elliptic Curves in Cryptography". Advances in Cryptology CRYPTO'85, New York, Springer-Verlag