A STUDY ON ELLIPTIC CURVE, ITS PROPERTIES AND APPLICATIONS

Bipin Chandra Upadhyay* Priyanka Sirola**
Assistant Professor, Dehradun Institute of Technology, Dehradun
M.Tech Scholar, Graphic Era Hill University Dehradun

ABSTRACT
Elliptic curve cryptography (ECC) is a kind of public key cryptosystem. In this paper, we will present some ECC algorithms and also give mathematical explanations on the working of these algorithms. Also we will discuss Elliptic curve in its application in digital signature generation and verification so as to securely transmit the data across different users.

Keywords: Cryptography, Digital Signature, ECDSA, elliptic curves.

1.INTRODUCTION
Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz [1] and Victor S. Miller [2] in 1985. Elliptic Curve Cryptography (ECC) is an asymmetric key cryptography. In asymmetric key cryptography each user generally has a pair of keys (a public key and a secret private key). The private key is the secret parameter of a particular user whereas the public key is distributed among all users taking part in the communication. Public key algorithms require a set of constants that should be predefined. For example Domain parameters in ECC. Asymmetric key cryptography, unlike symmetric key cryptography, does not require any shared secret key between the sender and receiver but is quite slower than symmetric key cryptography. [3]

2.BACKGROUND

2.1 Cryptography
As we all know information needs to be secured from attacks. Security is the most important feature in all area of communication. While sending a message to a person over channel such as internet we must provide confidentiality, integrity, authenticity and non-repudiation. These are the four major security aspects [4] or goals. Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption) - a process of transforming information using some technique to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Encryption was used to ensure confidentiality in communications.

2.2 Digital Signature
Signature is a method to authenticate any document. It is a proof to the recipient that the document comes from the correct entity (sender). In the present world most of the documents are electronic due to the trendy usage of the computer and its applications like email, e-banking, e-commerce, etc. Thus the message, data, documents or any other materials in electronic format as to be signed electronically. His signature that is done electronically is known as Digital Signature. [4, 5].
2. ELLIPTIC CURVE CRYPTOGRAPHY

3.1 Introduction to elliptic curves

In mathematics, an elliptic curve is a smooth, projective algebraic curve of genus one, on which there is a specified point $O$. An elliptic curve is in fact an Abelian variety — that is, it has a multiplication defined algebraically with respect to which it is a (necessarily commutative) group — and $O$ serves as the identity element. Often the curve itself, without $O$ specified, is called an elliptic curve. Any elliptic curve can be written as a plane algebraic curve defined by an equation of the form:

$$y^2 = x^3 + ax + b \quad \text{(3.1)}$$

which is non-singular; that is, its graph has no cusps or self-intersections. (When the characteristic of the coefficient field is equal to 2 or 3, the above equation is not quite general enough to comprise all non-singular cubic curves; see below for a more precise definition.) The point $O$ is actually the "point at infinity" in the projective plane.

3.1.1 Elliptic Curve over prime numbers

An elliptic curve over a field $K$ is a non-singular projective algebraic curve over $K$ with genus 1 together with a given point, $O$. Having given this high powered definition we will know proceed to ignore it and try to explain elliptic curves in a manner that is understandable (with some suspension of disbelief) by anyone who knows high school algebra and geometry.

We can understand an elliptic curve as all the points on the curve (given by the Weirstrass equation)

$$Y^2 + a_1XY + a_3Y = x^3 + a_3x^2 + a_4x + a_5 \quad \text{(3.2)}$$

together with $O$, the “point at infinity”. We also require that the curve is nonsingular, so has no cusps or self intersections. An example is shown in Fig 3.1, where we consider the point at infinity to be the point infinitely far to the top and bottom of the graph. Note that if the field we are working over has characteristic not equal to two or three then we can make a change of variables (for example could complete the square with y’s on the left hand side since could divide by two) to convert our Weirstrass equation to

$$Y^2 = x^3 + ax + b \quad \text{(3.3)}$$

An elliptic curve forms an abelian group. An abelian group, also called a commutative group, is a group in which the result of applying the group operation to two group elements does not depend on their order. Abelian groups generalize the arithmetic of addition of integers.[4,5] An abelian group is a set, $A$, together with an operation "$\cdot$" that combines any two elements $a$ and $b$ to form another element denoted $a \cdot b$. The
symbol "•" is a general placeholder for a concretely given operation. To qualify as an abelian group, the set and operation, \((A, \bullet)\), must satisfy five requirements known as the abelian group laws:

**Closure**: For all \(a, b \in A\), the result of the operation \(a \bullet b\) is also in \(A\).

**Associativity**: For all \(a, b\) and \(c \in A\), the equation \((a \bullet b) \bullet c = a \bullet (b \bullet c)\) holds.

**Identity element**: There exists an element \(e \in A\), such that for all elements \(a \in A\), the equation \(e \bullet a = a \bullet e = a\) holds.

**Inverse element**: For each \(a \in A\), there exists an element \(b \in A\) such that \(a \bullet b = b \bullet a = e\), where \(e\) is the identity element. Commutativity: For all \(a, b \in A\), \(a \bullet b = b \bullet a\).

To define these group laws consider two points, \(P\) and \(Q\), on our elliptic curve and draw the line from \(P\) to \(Q\) until you hit the curve again. This forms another point on the curve. This line intersects the elliptic curve again is \(P + Q\). This definition is perfectly general but if \(P = Q\) or one of \(P\) and \(Q\) equals \(O\) then it takes some interpreting. Because we only have one point at infinity we can usually get away with considering \(O\) as a special case. If we are trying to find \(2P\), then \(P\) and \(Q\) are the same point. In this case we take the line between \(P\) and \(Q\) to be the tangent line at \(P\) and proceed in the same manner as above. If the line from \(P\) to \(Q\) doesn’t intersect the curve anywhere on the finite plane (in our figures this means the line is vertical) then we say that it intersects the elliptic curve at \(O\) – this is why we needed to include this point on our curve. Then the line from \(O\) to \(O\), the “line at infinity”, intersects the curve at \(O\). Thus \(P + Q = O\). The line between \(P\) and \(Q\) is the same as the line between \(Q\) and \(P\) so \(P + Q = Q + P\). Also if we want to calculate \(P + O\) then the line between these two points is the same as the line between \(O\) and the point where the first line intersects the curve. This means \(P + O = P\) and \(O\) is the identity of our group. Fig 3.2 shows these properties.

**Algorithm 3.1.** Let \(E\) be an elliptic curve given by
\[ Y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5. \]
(a) If \(P_0 = O\) then \(-O = O\). Otherwise let \(P_0 = (x_0, y_0) \in E\). Then
\[ -P_0 = (x_0, -y_0 - a_1x_0 - a_3). \]
(b) If one of \(P_1\) or \(P_2\) equals \(O\) then use \(P + O = O + P = P\), otherwise let
\[ P_1 + P_2 = P_3 \text{ with } P_i = (x_i, y_i) \in E. \]
If \(x_1 = x_2\) and \(y_1 + y_2 + a_1x_2 + a + 3 = 0\)
then \(P_1 + P_2 = O\). Otherwise, let
\[ \lambda = (y_2 - y_1)/(x_2 - x_1), \text{ and} \]
\[ \nu = (y_1x_2 - y_2x_1)/(x_2 - x_1) \text{ if } x_1 \neq x_2; \text{ .......... (3.4) } \]
and
\[ \lambda = (3x_1^2 + 2a_2x_1 + a_4 - a_1y_1)/(2y_1 + a_1x_1 + a_3) \text{ .......... (3.6)} \]

Now draw a line from the point at infinity, \(O\), through this new point. The point where this line intersects the elliptic curve again is \(P + Q\).
\[ v = \left( -x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1 \right) / \left( 2y_1 + a_1 x_1 + a_3 \right) \]

if \( x_1 = x_2 \)............ (3.7)

(So \( y = \lambda \ x + v \) is the line through \( P_1 \) and \( P_2 \), or tangent to \( E \) if \( P_1 = P_2 \).)

Then \( P_3 = (x_3, y_3) \) where

\[ x_3 = \lambda^2 + a_1 \lambda - a_2 - x_1 - \]

\[ x_2 \] ................. (3.8)

\[ y_3 = - (\lambda + a_1)x_3 - v - a_3 \] ....... (3.9)

With this definition of addition we can (almost) show that the points on an elliptic curve define a abelian group.

**Theorem 3.1.** The addition law on an elliptic curve, \( E \), as given in Algorithm 3.1, has the following properties:

1. \( P + O = P \) for all \( P \in E \).
2. \( P + Q = Q + P \) for all \( P, Q \in E \).
3. Let \( P \in E \). There is a point of \( E \), denoted \( -P \), so that \( P + (-P) = O \)............. (3.10)
4. Let \( P, Q, R \in E \). Then \( (P + Q) + R = P + (Q + R) \)........... (3.11)

In other words, the addition law makes \( E \) into an abelian group with identity \( O \).

**Proof.**

Associativity is the only hard part of this proof.

1. By definition.
2. The addition formulae given above are symmetrical. If you swap \( P_1 \) and \( P_2 \) then \( \lambda \) and \( v \) remain the same.

3. \( -P \) is defined above and has this property.

4. The three options are to: convince yourself geometrically, take three points on \( E \) and construct their sum in the two different ways.

Alternatively you could take three general points and add them in the two different ways using the explicit addition formulae.

The problem with this is you have to consider all the different cases depending on whether any of the points \( P, Q \) and \( R \) are equal. Probably the most enlightening proof is by the Riemann–Roch Theorem, as in [6].

In this proof it is obvious that the object we define a group but it is not so obvious that it is an elliptic curve. However this would take us too far afield so we leave this as just a suggestion of a proof.

5. If \( P_1, P_2 \in E(K) \) then we can see that \( P_1 + P_2 = (x_3, y_3) \) where the coordinates are given by rational functions (quotients of polynomials) in the variables \( x_1, y_1, a_i \), all of which are in the field \( K \). This means that \( x_3, y_3 \in K \), that is \( P_1 + P_2 \in E(K) \). Therefore \( E(K) \) is a subgroup of \( E \).

**3.1.2 Elliptic curves over finite fields**

We can consider an elliptic curve defined over a finite field, which will turn out to have a finite number of points, which we can in fact bound. Our first example comes from [7].

**Theorem 3.2 (Hasse’s theorem).** Let \( E \) be an elliptic curve over the finite field \( F_q \). If \( E(F_q) \) has order \( N \) we have \( |N - (q + 1)| \leq 2\sqrt{q} \).

Hasse’s theorem gives us a fairly tight bound on the number of points on an elliptic curve over a finite field. However we will see later that it is sometimes important to know exactly how many points there are.
The most efficient current algorithm to find this is Schoof’s point counting algorithm, invented in 1985 by Schoof. It can compute the number of points on an elliptic curve over a finite field $F_q$ in at most a constant times $\log_8 q$ operations. This algorithm is fairly complicated but allows us to calculate the number of points on $E(F_q)$ for $q$ with several hundred decimal digits.

3.2 Discrete Logarithm Problem

If $p$ is a prime number, then $Z_p$ denotes the set of integers $0, 1, 2, \ldots, p - 1$, where addition and multiplication are performed modulo $p$. It is well-known that there exists a non-zero element $\alpha \in Z_p$ such that each non-zero element in $Z_p$ can be written as a power of $\alpha$ such an element $\alpha$ is called a generator of $Z_p$. The discrete logarithm problem (DLP) [8] is the following: given a prime $p$, a generator $\alpha$ of $Z_p$, and a non-zero element $\beta \in Z_p$, find the unique integer $k, 0 \leq k \leq p-2$, such that $\beta \equiv \alpha^k \pmod{p}$. The integer $k$ is called the discrete logarithm of $\beta$ to the base $\alpha$.

3.2.1 Elliptic Curve Discrete Logarithm Problem

The classical or general DLP(discrete logarithm problem) is the following:

If $b \equiv a^k \pmod{p}$, where $p$ is prime and $k$ is any random integer. DLP is the problem to find $k$. Similarly, ECDLP is the discrete log problem for elliptic curves. i.e. If $kP = Q$, where $P, Q$ are points on the curve $E_p(a, b)$ and $k$ is an integer such that $Q$ lies on the curve ECDLP is the problem of finding $k$ knowing $P$ and $Q$.

**Notations:** $E(F_q)$ is the set of all points on $E$ whose all coordinates lie in $F_q$.

$F_q$ denotes $F_p^n$. Difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP) decides the security of ECC-based signature. The high computational complexity of ECDLP is the reason of ECC-based signatures being more secured than other cryptosystems-based signature. Since ECDLP is much tougher to solve than DLP, the attacker first converts the ECDLP to DLP in most of the attacks.

4. ELLIPTIC CURVE AND DIGITAL SIGNATURE

This is one of the algorithm that is used for authentication of a message between 2 clients (Let the clients be A and B). A has to sign the message using its private key to authenticate a message sent by A. A sends the message and the signature to B. This signature can be verified only by using the public key indeed send by A. [4, 5] This is a variant of the Digital Signature Algorithm (DSA). It operates on elliptic curves. Both the clients have to agree up on Elliptic Curve domain parameters to send a signed message from one to the other. Sender A has a key pair - a private key $d$(a randomly generated integer less than $n$, where $n$ is the order of the curve) and a public key $Q = d * G$(G is the base point). An overview of ECDSA process is defined below.

4.1 ECC Domain Parameters

Elliptic curve cryptography (ECC) domain parameters over $GF(P)$, can be represented by a six tuple:

$E = (q, a, b, G, n, h)$, where

$q = P$ or $q = 2m$, where $m$ is a natural number.

$a$ and $b$ are the co-efficients of $x^3$ and $x$ respectively used in the equation.

$y^2 \equiv x^3 + ax + b \pmod{P}$ for $q = P \geq 3$

$y^2 + xy = x^3 + ax^2 + b$ for $q = 2m \geq 1$

$G$ is a base point on the elliptic curve.

$n$ is prime number which is of the order of $G$. The order of a point on an elliptic curve is the smallest positive integer $r$ such that $rP = 0$.
Finally \( h = |E| / n \), where \( |E| \) represents the total number of points on elliptic curve and it is called the curve order.

### 4.2 Elliptic Curve Digital Signature Algorithm (ECDSA)

The elliptic curve digital signature algorithm (ECDSA) was proposed by Abdalla, Bellare and Rogaway in 1999 [5, 9]. Entity \( A \) has domain parameters \( D = (q, a, b, G, n, h) \) and public key \( Q_a \) and private key \( d_a \). And entity \( B \) has authentic copies of \( D \) and \( Q_a \). To sign a message \( m \), \( A \) does the following:

#### 4.2.1 Signature Generation

- Select a random integer \( k \) from \([1, n-1]\).
- Compute \( kG = (x_1, y_1) \) and \( r = x_1 \mod n \). If \( r = 0 \) then go to step 1.
- Compute \( k^{-1} \mod n \). Compute \( e = \text{hash}(m) \).
- Compute \( s = k^{-1} e + d_a \cdot r \mod n \). If \( s = 0 \) then go to step 1.

\( A \)'s signature for the message \( m \) is \((r, s)\).

#### 4.2.2 Signature verification

Verify that \( r \) and \( s \) are integers in \([1, n-1]\).

- Compute \( e = \text{hash}(m) \).
- Compute \( w = s^{-1} \mod n \).
- Compute \( u_1 = e \cdot w \mod n \) and \( u_2 = r \cdot w \mod n \).
- Compute \( (x_1, y_1) = u_1 G + u_2 Q_a \).
- Compute \( v = x_1 \mod n \). Accept the signature if and only if \( v = r \). SHA-1 denotes the 160-bit hash function.

### 5. APPLICATION OF ECC

Smart card [10] is a very good example where ECC can be applied. These are used in a wide variety of applications such as e-commerce, identification and many more. It is really advantageous if we use asymmetric key cryptography for short messages.

### Table 4.1: A comparison of key sizes needed to achieve equivalent level of security with three different methods

<table>
<thead>
<tr>
<th>Symmetric Encryption</th>
<th>RSA and Diffie-Hellman</th>
<th>Elliptic Curve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key size in bits</td>
<td>Key size in bits</td>
<td>Key size in bits</td>
</tr>
<tr>
<td>80</td>
<td>1024</td>
<td>160</td>
</tr>
<tr>
<td>112</td>
<td>2048</td>
<td>224</td>
</tr>
<tr>
<td>128</td>
<td>3072</td>
<td>256</td>
</tr>
<tr>
<td>192</td>
<td>7680</td>
<td>384</td>
</tr>
<tr>
<td>256</td>
<td>15360</td>
<td>512</td>
</tr>
</tbody>
</table>

The most important constraints from the programmer's point of view are the limited RAM, ROM and EEPROM available, and the requirement to limit the processing time. A typical inexpensive smart card has between 128 and 1024 bytes of RAM, 4 and 16 Kbytes of EEPROM, and 16 and 32 Kbytes of ROM. The CPU is typically 8-bit and clocked at 3.57 MHz [7]. Any addition to memory or processing capacity increases the cost of the card. It is certainly not acceptable to use all resources available on the smart card to implement the cryptographic services. So it is better to use ECC on smart card which uses smaller key size. Table 4.1 shows a comparison of key sizes of different cryptosystems. From this it is clear that ECC gives same level of security with a smaller key size as compare to others. But we must choose the ECC parameters carefully.

### 6. CONCLUSION

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. This paper gives a...
crystal clear picture of ECC and digital signature application of it, ECC’s advantages and some application of ECC like ECDSA. The demonstration included some of the theoretical and practical aspects of ECC.

7. REFERENCES