Enhancing Security to the Information Using 3D Geometric Algebra Properties to Elliptic Curve Cryptography

J. Chakradhar
Research and Development, Sri Venkatesa Perumal College of Engineering and Technology
R.V.S. Nagar, Puttur, Andhra Pradesh
www.chakri.info
jalakamchakradhar@gmail.com

ABSTRACT
In ECC (Elliptic Curve Cryptography) algorithm we use only elliptic curves. This paper gives an idea of enhancing ECC in two aspects. One is using of all symmetric curves from two dimensional geometry to the place of elliptic curve and another one is using three dimensional coordinates for elliptic curves. For using of all symmetric curves we are defining a new algebraic structure with three elements \([G, i, o]\) Here \(G\) is collection of vertices of a figure. And “i” is identity element basing on the symmetric axis and “o” is an operation basing on the operation. “All the points’ lies on a symmetrical curve (2D) or on a symmetrical object (3D) forms an ABELIAN with respect to some operation” has to be proved

KEYWORDS
The terms cryptography and cryptology are interchangeably in English. Cryptography refers to specifically the use and practice of cryptographic techniques and Cryptology refer to the combined study of cryptography and cryptanalysis. Cryptography is the practice and study of hiding information. Elliptic curve is a smooth, projective algebra curve. The genus of a connected, orientable surface is an integer representing the maximum number of cuttings along non-intersecting closed simple curves without rendering the resultant manifold disconnected. Abelian group – an algebraic structure that satisfies closure, associative, commutative properties and there exists identity an there exists inverse to each element in that set.

INTRODUCTION

1. ELLIPTIC CURVES
1.1 DIFFERENT ELLIPTIC CURVES
In mathematics, an elliptic curve is a smooth, projective algebra curve, on which there is a specified point \(O\). An elliptic curve is in fact an abelian that is, it has a multiplication defined algebraically with respect to which it is an abelian 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 \(y^2 = x^3 + ax + b\)

Which is non-singular; that is, its graph has no curves 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)The point \(O\) is actually the "point at infinity" in the projective plane.
If \(y^2 = P(x)\), where \(P\) is any polynomial of degree three in \(x\) with no repeated roots, then we obtain a nonsingular plane curve, which is thus also an elliptic curve. If \(P\) has degree four and is square free this equation again describes a plane curve of genus one; however, it has no natural choice of identity element. More generally, any algebraic curve of genus one, for example from the intersection of two three-dimensional quadric surfaces, is called an elliptic curve, provided that it has at least one rational point.

1.2 ELLIPTIC CURVES OVER THE REAL NUMBERS
Although the formal definition of an elliptic curve is fairly technical and requires some background in algebraic geometry, it is possible to describe some features of elliptic curves over
the real numbers using only high school algebra and geometry.

Graphs of curves $y^2 = x^3 - x$ and $y^2 = x^3 - x + 1$ in this context, an elliptic curve is a plane curve defined by an equation of the form $y^2 = x^3 + ax + b$
Where $a$ and $b$ are real numbers. This type of equation is called a Weierstrass equation.

The definition of elliptic curve also requires that the curve be non-singular. Geometrically, this means that the graph has no cusps or self-intersections. Algebraically, this involves calculating the discriminant $\Delta = -16(4a^3 + 27b^2)$
The curve is non-singular if and only if the discriminant is not equal to zero. (Although the factor $-16$ seems irrelevant here, it turns out to be convenient in a more advanced study of elliptic curves.) The (real) graph of a non-singular curve has two components if its discriminant is positive, and one component if it is negative. For example, in the graphs shown above, the discriminant in the first case is 64, and in the second case is $-368$.

1.3 THE GROUP LAW

By adding a "point at infinity", we obtain the projective version of this curve. If $P$ and $Q$ are two points on the curve, then we can uniquely describe a third point which is the intersection of the curve with the line through $P$ and $Q$. If the line is tangent to the curve at a point, then that point is counted twice; and if the line is parallel to the $y$-axis, we define the third point as the point "at infinity". Exactly one of these conditions then holds for any pair of points on an elliptic curve.

It is then possible to introduce a group operation, "$+$", on the curve with the following properties: we consider the point at infinity to be $0$, the identity of the group; and if a straight line intersects the curve at the points $P$, $Q$ and $R$, then we require that $P + Q + R = 0$ in the group. One can check that this turns the curve into an abelian group, and thus into an abelian variety. It can be shown that the set of $K$-rational points (including the point at infinity) forms a subgroup of this group. If the curve is denoted by $E$, then this subgroup is often written as $E(K)$.

The above group can be described algebraically as well as geometrically. Given the curve $y^2 = x^3 - px - q$ over the field $K$ (whose characteristic we assume to be neither 2 nor 3), and

If $x_P = x_Q$, then there are two options: if $y_P = -y_Q$, including the case where $y_P = y_Q = 0$, then the sum is defined as $0$; thus, the
inverse of each point on the curve is found by reflecting it across the x-axis. If \( y_p = y_q \neq 0 \), then \( R = P + P = 2P = (xR, -y_R) \) is given by

\[
P = (2.35, -1.86), \quad Q = (0.1, 0.836), \quad -R = (3.89, 5.62), \quad R = (3.89, -5.62)
\]

\[
P + Q = R = (3.89, -5.62).
\]

2. ENCRYPTIO
An elliptic curve is a plane curve which consists of the points satisfying the equation \( y^2 = x^3 + ax + b \) along with a distinguished point at infinity, denoted \( O \). This set forms an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety.

As for other popular public key cryptosystems, no mathematical proof of difficulty has been published for ECC as of 2009. However, the U.S. National Security Agency has endorsed ECC technology by including it in its Suite B set of recommended algorithms and allows their use for protecting information classified up to top secret with 256-bit keys. Although the RSA patent has expired, there are patents in force known theorems & results on groups, subgroups, cyclic groups, cosets, normal subgroups and well each element and commutative) to all remaining properties like definition (closure, associative, existence of identity, inverse to operation which may change basing on this inverse element.

There is a particular result in 2D geometry that is “the points lie on a symmetrical shape forms an abelian with respect to some operation”. For each elliptic curve there should be a symmetric axis. In the similar way we can extend the above result by defining “the points lie on a symmetrical shape forms an abelian with respect to some operation”. Now let us look at the encryption process in Elliptic Curve Cryptography.

Take the prime \( p = 751 \) and

Elliptic Curve is \( y^2 = x^3 - x + 188 \).

So \( a = -1 \) and \( b = 188 \), \( E_p(a, b) = E_{751}(-1, 188) \)

\( G = (0, 376) \)

Suppose that Sender wishes to send a message \( m \) to the Receiver that is encoded in the Elliptic point \( P_m = (562, 201) \) this point lies on the curve \( y^2 = x^3 - x + 188 \) and suppose the Sender selects the random number \( k = 386 \).

Receiver’s public key is \( P_k = (201, 5) \). We have 386(0, 376) = (676, 558) and (562, 201) + 386(201, 5) = (385, 328)

In the above explanation we are using only 2D so the coordinates are of (X, Y) only.

To Enhancing Security to the information we use 3D Geometric Algebra properties to Elliptic curve cryptography so the coordinates are having one more coordinate that is z-coordinate.

3. D GEOMETRIC ALGEBRA
The new algebraic structure \((G, i, o)\) has to be characterised\(^1\). Where

\( G \) gathering of elements – vertices of a figure.

Identity element – one vertex this depends upon symmetric axis.

Operation – operation may change basing on this inverse element.

The above is for two dimensional geometrical algebra. This can be extended for three dimensional. So we have to develop\(^2\) one more algebraic structure for 3D.

After that, the statement “All the points lie on a symmetrical curve (2D) or on a symmetrical object (3D) forms an ABELIAN” has to be proved\(^3\).

Then the applicability of encryption in such a way as in Elliptic curve cryptography leads to produce more and more different strong encryption algorithms.

4. CONCLUSION
While proving the above said three statements will give a lot of essence to the researchers. The first one ‘characterising means to check out all the properties of group theory that is from basic definition (closure, associative, existence of identity, inverse to each element and commutative) to all remaining properties like subgroups, cyclic groups, cosets, normal subgroups and well known theorems & results on groups. The second statement, to develop means to develop 3D algebraic structure and to check all the above properties. The third one is a universal result. If it is already proved then it can be used directly. Otherwise we have to get it finished.

REFERENCES

[5]. J.Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjolsns, F. Muller, T.Pedersen, B. Ptzmann, P. de Rooij,


AUTHOR
J. Chakradhar did Diploma in Computer’s, B.Tech in Information Technology (IT), Received M.Tech in Computer Science and Engineering (CSE) from J.N.T. University, Ananthapur and Now Perusing Ph.D in Computer Science and Engineering. He worked as IT specialist for IBM; He proposed IT optimization solutions for many reputed organizations. He is a Microsoft certified System Administrator (MCSA), Sun certified System Administrator (SCSA), Ankit fadia Certified Ethical Hacker (AFCEH) Currently he is working as Research and Development In charge, S.V.P.C.E.T., J.N.T.U.A. His area of interest includes Computer Networks, Network Security, Information Security, Operating Systems. He has published several papers in National and International journals and conferences. He is life member of different professional societies like Indian Society of Technical Education (ISTE), Computer society of India (CSI), Internet Society (ISOC). For Detailed profile visit www.chakri.info