# A Discussion on Elliptic Curve Cryptography and its Application

Ajit karki[1], Sandeep Gurung[2] and Kiran Gautam[3]
[1, 2,3]*Department of computer Science & Engineering, Sikkim Manipal Institute Of Technology, Majhitar, Sikkim, India*
[1]*ajitkarki4@gmail.com*,[2]*gurung_sandeep@yahoo.co.in*, [3]*kiran.gautam.cse@gmail.com*

**Abstract-** Cryptography is an important part of preventing private data from being stolen. Even if an attacker were to break into your computer or intercept your messages they still will not be able to read the data if it is protected by cryptography or encrypted. In addition to concealing the meaning of data, cryptography performs other critical security requirements for data including authentication, repudiation, confidentiality, and integrity. 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. The Crux of cryptography lies in the key involved and the secrecy of the keys used to Encrypt or decrypt. Another important factor is the key strength, i.e. the size of the Key so that it is difficult to perform a brute force on the plain and cipher text and retrieve the key. There have been various cryptographic algorithms suggested. Elliptic curve cryptography (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, a 160 bit ECC has roughly the same security strength as 1024 bit RSA). In this paper, we will present some ECC algorithms and also gives mathematical explanations on the working of these algorithms.

**Keywords:** Elliptic Curve, cryptography, cryptosystem, RSA.

## 1. Introduction

Elliptic curve cryptography was introduced in the mid-1980s 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. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. 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
  $y^2 = x^3 + ax + b$.

  Examples:

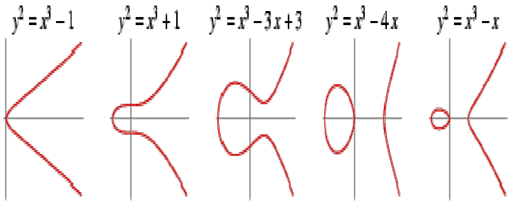

Figure: General form of EC [1].

## 2. Domain parameters

There are certain public constants that are shared between parties involved in secured and trusted ECC communication. This includes curve parameter **a**, **b**, a generator point **G** in the chosen curve, the modulus **p**, order of the curve **n** and the cofactor **h**. There are several standard domain parameters defined by SEC, Standards for Efficient Cryptography [4].

### *2.1. Key Generation* :

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt it's with private key.

Now, we have to select a number**'d'** within the range of **'n'**.

Using the following equation we can generate the public key

Q = d * P

**d** = the random number that we have selected within the range of (**1 to n-1**). **P** is the point on the curve.

'Q' is the public key and'd' is the private key.

### *2.1.1 Encryption:*

Let 'm' be the message that we are sending. We have to represent this message on the curve.

Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 - (n-1)].

Two cipher texts will be generated let it be C1 and C2.

C1 = k*P

C2 = M + k*Q

C1 and C2 will be sending.

### *2.1.2 Decryption:*

We have to get back the message 'm' that was send to us,

M = C2 – d * C1

M is the original message that we have send.

**Proof:**

How do we get back the message?

M = C2 – d * C1

'M' can be represented as 'C2 – d * C1′

C2 – d * C1 = (M + k * Q) – d * (k * P)   (C2 = M + k * Q and C1 = k * P)

= M + k * d * P – d * k *P   (canceling out k * d * P)

= M (Original Message)

***2.2. Point addition:*** Point addition is defined as taking two points along a curve *E* and computing where a line through them intersects the curve. The negative of the intersection point is used as the result of the addition. The operation is denoted by P+Q=R.

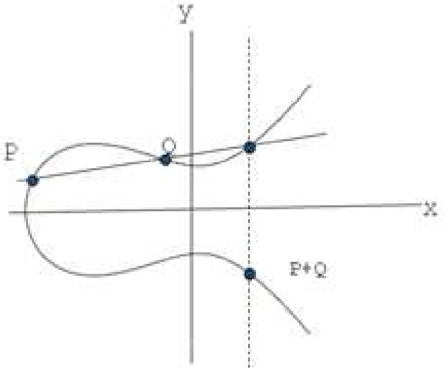

Figure 1: Elliptic Curve Point addition operation [1].

### *2.3. Point multiplication*

In point multiplication a point P on the elliptic curve is multiplied with a scalar k using elliptic curve equation to obtain another point Q on the same elliptic curve. i.e. kP=Q

Point multiplication is achieved by two basic elliptic curve operations

- Point addition, adding two points J and K to obtain another point L i.e., L = J + K.
- Point doubling, adding a point J to itself to obtain another point L i.e. L = 2J.

Point addition and doubling are explained in sections Point Addition and Point Doubling respectively, here is a simple example of point multiplication. Let P be a point on an elliptic curve. Let k be a scalar that is multiplied with the point P to obtain another point Q on the curve. i.e. to find Q = kP. If k = 23 then kP = 23.P = 2(2(2(2P) + P) + P) + P.

Thus point multiplication uses point addition and point doubling repeatedly to find the result. The above method is called double and add' method for point multiplication. [1].

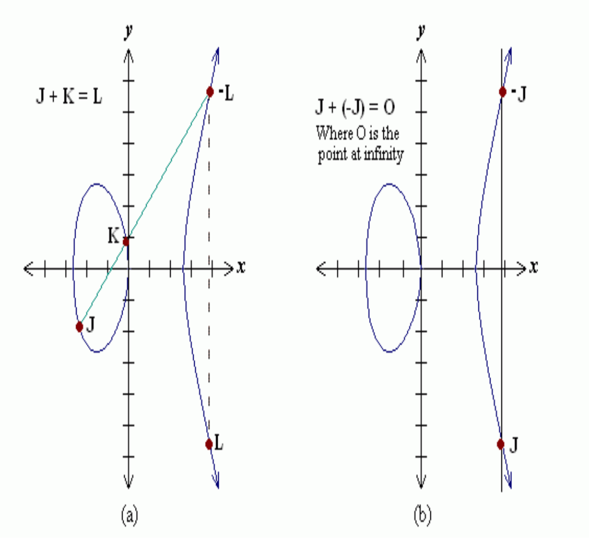

Figure 2: (a) Point addition, (b) Point multiplication. [3]

## 3. An EC cryptographic algorithm for key agreement is explained below.

***3.1 Elliptic curve Diffie Hellman (ECDH): Elliptic curve Diffie–Hellman (ECDH)*** is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public–private key pair, to establish a shared secret over an insecure channel. This shared secret may be directly used as a key, or better yet, to derive another key which can then be used to encrypt subsequent communications using a symmetric key cipher. It is a variant of the Diffie–Hellman protocol using elliptic curve cryptography.

- Diffie-Hellman (DH) public-key algorithm.

Diffie-Hellman was the first public-key algorithm ever invented, way back in
1976. It gets its security from calculating discrete logarithms in a finite field. The
idea behind Diffie-Hellman algorithm is to generate a private key that can later be
used for communication, and sharing it in a secure fashion.

- Two phases:
  - ➢ I phase setup

E: $y^2 = x^3 + ax + b \bmod P$

Primitive element P= (xp,yp)

- ➢ II phase: protocol.

Ajay                    Bijay

a=KprA $\in$ {2,3,….#E}    b=Kpr B $\in$ {2,3,….#E}
A=KpubA=a.p=(xA,yA)    B=KpubB=b.p=(xB ,yB)

a.B= (xAB,yAB)    b.A=(xAB,yAB)

- Now encrypt the message
- Message m

**Proof of correctness:**
Ajay computes
a.B = a (b.p) =abp
Bijay computes
b.A=b(a.p)=abp

How to compute a.p = p+p+p+p+….p (a times)
The point multiplication a.p can be computed with “double and add algorithm”.
Ex: 26p=??

- 26P=(110102)P

Steps:
0 p= 1 time p
Left to right method:

|  |  |  |
|---|---|---|
| 1a | P + P=2P=$10_2$P | D |
| 1b | 2P+P=3P= $11_2$P | A |
| 2a | 3P+3P =6P=$110_2$P | D |
| 3a | 6P+6P=12P=$1100_2$P | D |
| 3b | 12P+P=13P=$1101_2$P | A |
| 4a | 13P+13P=26P=$11010_2$P | D |

## 4. The ECC Advantages

It is worthy to note that a 160-bit ECC key has about the same level of security as a 1024-bit RSA key. The most important difference between ECC and other conventional cryptosystems is that for a well-chosen curve, the best method currently known for solving the ECDLP is fully exponential, while sub-exponential algorithms exist for conventional cryptosystems. This difference largely contributes to the huge disparity in their respective running times. It also means that ECC keys have much fewer bits than IFP and DLP based applications. ECC keys take much more effort to break compared to RSA and DSA keys. Due to this, many people believe that ECDLP is intrinsically harder than the other two problems. While this deduction might be true, we have no way of proving it. We do not know if a fast and efficient elliptic curve DL algorithm that runs in sub-exponential time will be discovered, say, in the next ten years, or if another class of weak curves will be identified that could compromise the security of elliptic curve cryptosystems. But one thing is certain. After years of intensive study, there is currently no faster way to attack the ECDLP other than fully exponential algorithms.

### *4.1 ECC Applications*

When the ECC was first introduced in 1985, there was a lot of skepticism about its security. However, ECC has since come a long way. After nearly a decade of serious study and scrutiny, ECC has yielded highly efficient and secure. Presently, many product vendors have incorporated ECC in their products, and this number has only been on the rise. Uncertainty still exists among some proponents of traditional cryptographic systems, but they are starting to become more accepting of this promising new technology. RSA Security Inc., for example, has long voiced concern regarding the security of ECC since its introduction. In recent years, however, RSA Security has researched on efficient ECC algorithms, and even acquired a patent on a storage-efficient basis conversion algorithm. Moreover, it has also integrated ECC into some of its products, acknowledging the fact that ECC has begun to establish itself as both secure and efficient. The factor is the strong promotion of the use of ECC through a Canadian-based Certicom Corporation. Certicom is a company that specializes in information security solutions in a mobile computing environment through providing software and services to its clients. Over the years, Certicom has published numerous papers in support of ECC and has also implemented ECC in all of its commercial products. Its success prompted many other companies to look more closely at the benefits and security of ECC. Now, ECC is becoming the mainstream cryptographic scheme in all mobile and wireless devices. Below is a short survey of ECC applications seen on the market today. Results of the survey can be broadly divided into some categories: smart cards, PDAs and PCs.

- **Smart Cards**

Smart cards are one of the most popular devices for the use of ECC. Many manufacturing companies are producing smart cards that make use of elliptic curve digital signature algorithms. These manufacturing companies include Phillips, Fujitsu, MIPS Technologies and DataKey, while vendors that sell these smart cards include Funge Wireless and Entrust Technologies. Smart cards are very flexible tools and can be used in many situations. For example, smart cards are being used as bank (credit/debit) cards, electronic tickets and personal identification (or registration) cards.

- **PDAs**

PDAs are considered to be a very popular choice for implementing public key cryptosystems because they have more computing power compared to most of the other mobile devices, like cell phones or pagers. However, they still suffer from limited bandwidth and this makes them an ideal choice for using ECC. In the January of 1998, 3Com4 Corporation teamed up with Certicom to implement ECC in future versions of its Palm Pilot organizer series and Palm Computing platform. This new feature will provide protection of confidential information on the hand-held organizers, user authentication in wireless communications and e-commerce transactions, and also ensure data integrity and proof of transactions.

- **PCs**

Constrained devices have been considered to be the most suitable platforms for implementing the ECC. Recently, several companies have created software products that can be used on PCs to secure data, encrypt e-mail messages and even instant messages with the use of ECC. PC Guardian Technologies is one such company that created the Encryption plus Hard Disk and Encryption plus Email software products. The former makes use of both RSA and EC Diffie-Hellman while the latter makes use of a strong 233-bit ECC key to encrypt its private AES keys.

- The Top Secret Messenger software was developed by Encryption Software Inc. It encrypts the messages of some of the most popular instant messaging programs today, like ICQ and MSN. It can also be used with e-mail clients such as Microsoft Outlook and Outlook Express to encrypt e-mail messages. This product uses both private and public key cryptosystems, including a 307-bit key for its implementation of the ECC.

## 5. 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. 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. The proposed protocol for Authentication and key agreement is based on ECC, which is a public-key type. The public key cryptography concept solves the key distribution and storage problems. ECC came as a new alternative public key cryptosystem to provide security strength more than any known public key system using smaller key sizes. The smaller key sizes result in smaller system parameters, smaller public key certificates, faster implementations, lower power requirements. Therefore, ECC is the best choice to solve SMS security issues, since it provides acceptable performance in low power mobile devices with a high security level.

As mobile devices have less memory and processing power, ECC can be used for message security on mobile. Symmetric key algorithms can be used on such device, but the authentication of the message is not guaranteed, there is a requirement of secure channel for the transfer of the message along with the key devoid which there could be possibilities of intruder attack on the messages. Considering the present use of the conventional RSA cryptosystem, there is a lot of problem with the key size and the processing speed. When implementing RSA on these devices, smaller keys must be used to meet the memory capacity but this makes the encryption weak. ECC is useful not only in resource constrained environment like mobile, pager or smart card devices which have limited memory, limited processing capability and limited backup but also on powerful computers because it provides strong security with smaller key sizes. The key between the two parties can be shared in a common network and will not affect the security of the encrypted message due to its discrete logarithmic problem. ECC also provides authenticated transfer of the message as there is an end-to-end secure data transfer. Elliptic curve cryptography has moved from being an interesting theoretical alternative to being a cutting edge technology adopted by an increasing number of companies.

## 6. Acknowledgement

I owe my gratitude to many people who have contributed towards the completion of this article with their encouragement and support. I am truly indebted to my advisor/Guide, Mr.Sandeep Gurung, Associate Professor,(CSE Deptt.Sikkim Manipal Institute of Technology,Majhitar,Rangpo,Sikkim,India)for his patient guidance. I am thankful to my Guide Mr.Kiran Gautam Assistant Professor-I (CSE Deptt.Sikkim Manipal Institute of Technology,Majhitar,Rangpo,Sikkim,India) for his valuable support. I also thankful to my teacher's (Prof) (Dr.) Kalpana Sharma, ,

(CSE Deptt. SMIT, Sikkim, India),
Mr.Udit Kr.Chaktraborty,Associateprofessor
(CSE Deptt.SMIT,Sikkim India) for their inspiration.

## 7. References

[1] B.Schneier. Applied Cryptography. John Wiley and Sons, second edition, 2013.

[2] Cryptography and Elliptic Curves, koblitz, second edition, 2012.

[3] Julio Lopez and Ricardo Dahab, “An overview of elliptic curve cryptography”, May 2011.

[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.