2 Days International Conference on Recent Innovations in Engineering, Science, Humanities and Management
Dev Samaj College for Women, Ferozepur, Panjab (India) (ICRIESHM-17)
18th -19th March 2017, www.conferenceworld.in ISBN: 978-93-86171-33-7

APPLICATION OF ELLIPTIC CURVES IN CRYPTOGRAPHY-A REVIEW

Savkirat Kaur

Department of Mathematics, Dev Samaj College for Women, Ferozepur (India)

ABSTRACT

Earlier, the role of cryptography was confined to the transmission of data securely. With the development of internet and the increased use of resource constrained devices, the need was to build up cryptosystems which are faster as well as reliable. Elliptic Curve Cryptography (ECC) is the major advancement in the field of cryptography providing faster and secure methods for encryption. The foundation of ECC is the operation of scalar multiplication in elliptic curves over finite fields. ECC uses shorter key sizes as compared to the classic public key cryptosystems (e.g. RSA) thus providing faster communication methods. The intent of this paper is to discuss the basic arithmetic of elliptic curves and their role in elliptic curve cryptography.

Keywords: Elliptic curve, Point addition, Point doubling, Scalar multiplication, Protocol, Elliptic curve cryptography, RSA

I. INTRODUCTION

In 20th century, with the development of internet, the need was to have a cryptography technique which would not involve sharing the same keyword between two parties. In 1976, Whitfield Diffie and Martin Hellman proposed Diffie Hellman key exchange protocol, which was the foundation of Public Key Cryptosystem [1]. In 1977, this protocol was implemented in RSA Encryption technique. In 1985, another public key cryptosystem was developed on the basis of nature of elliptic curves in finite fields, named as Elliptic Curve Cryptography (ECC). The first use of elliptic curves in cryptography was recommended by Neal Koblitz and Victor S. Miller. ECC utilizes the methods of Diffie-Hellman Key Exchange and RSA Encryption, but in this system the prime numbers are selected with the help of an elliptic curve in a finite field [2, 3]. An elliptic curve over a field K is an algebraic curve in a plane and is represented by equation (1), as follows:

$$E: \quad y^2 = x^3 + lx + m \tag{1}$$

where, l & $m \in$ K and $4l^3 + 27m^2 \neq 0$

In other words, the set of points (x,y) which satisfy the above equation together with the point at infinity '$\mathcal{O}$' represent an Elliptic curve [4]. It can be observed that this set of points become an Abelian group under the composition defined in next section.

ISBN: 978-93-86171-33-7

II. GROUP OPERATIONS FOR ELLIPTIC CURVE

2.1 Point Addition

Elliptic curves form a group under the composition of point addition. The geometric and algebraic approach of this composition is discussed below.

2.1.1 Geometrical Approach

Given two points P (x_P, y_P) and $Q(x_Q, y_Q)$ in the set E = $\{(x, y): y^2 = x^3 + lx + m\}$ as shown in Fig.2.1.1 (a). If P ≠ -Q, then the composition is defined as P + Q = R where, –R is the point on the curve where the straight line joining the points P and Q meet the curve and R is the reflection of –R with respect to x-axis. If P = -Q, then the line through this point intersects at a point at infinity $\mathcal{O}$. In this case, P + (-P) = $\mathcal{O}$ as shown in Fig.2.1.1 (b). $\mathcal{O}$ is the additive identity of the group of points on the elliptic curve [5].

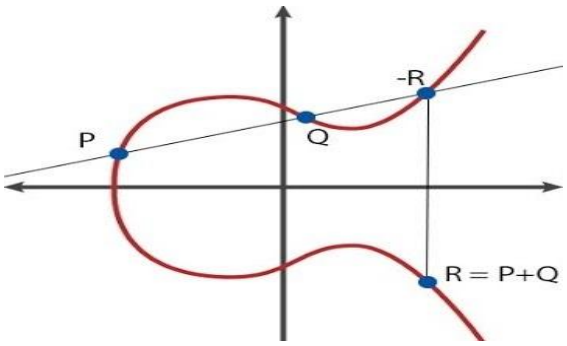

Fig.2.1.1 (a) point addition P ≠ -Q

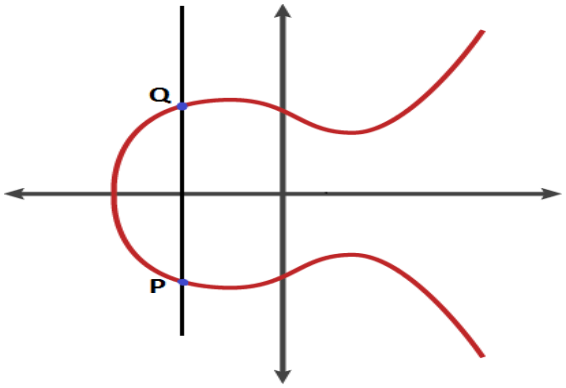

Fig.2.1.1 (b) point addition P = -Q

2.1.2 Algebraic Approach

The coordinates of the point –R are $(x_R, -y_R)$. Suppose S is the slope of the line joining the points P and Q, therefore S can be expressed by equation (2):

$$S = \frac{y_P - y_Q}{x_P - x_Q} = \frac{y_P + y_R}{x_P - x_R} = \frac{y_Q + y_R}{x_Q - x_R} \quad (2)$$

As the points P, Q and –R lie on the elliptic curve, therefore equation (1) implies the following equations:

$$\left\{ \begin{array}{l} y_P^2 = x_P^3 + lx_P + m \\ y_Q^2 = x_Q^3 + lx_Q + m \\ y_R^2 = x_R^3 + lx_R + m \end{array} \right\} \quad (3)$$

Further, the coordinates of R can be computed as:

$$x_R = S^2 - (x_P + x_Q)$$
$$y_R = S(x_P - x_R) - y_P \quad (4)$$

The operation defined above is also known as Point Addition [2]. Under this operation, elliptic curves satisfy all the properties of an abelian group.

2.2 Point Doubling

Point Doubling of a point P (x_P, y_P) is defined as the addition of the point to itself. If $y_P \neq 0$, then geometrically a tangent is drawn to the curve at that point. The point of intersection of the tangent with the curve is -2P and the reflection of -2P with respect to x axis is 2P. If $y_P = 0$, then doubling that point is the point at

ISBN: 978-93-86171-33-7

infinity $\mathcal{O}$ [2, 6]. In order to implement Diffie Hellman key exchange protocol, the group operation scalar multiplication is also required.

2.3 Scalar Multiplication

Scalar Multiplication is nothing but the repeated point addition. Given a point P (x_P, y_P) on the curve and any scalar k $\in Z$, the scalar multiplication is defined as:

$$Q = kP = P+P+P+.....+P \text{ (k times)}$$

The operation of scalar multiplication acts as a one way function for Diffie Hellman key exchange protocol [6, 7].

III. ELLIPTIC CURVE CRYPTOGRAPHY

3.1 Elliptic Curve Discrete Log Problem

Consider an elliptic curve over a finite field $Z/_{pZ}$. Given P $\in$ E ($Z/_{pZ}$) and a scalar k $\in Z$, it is easy to evaluate Q; where Q = kP. But if P and Q are given, it is very difficult to find the scalar k. This is the principle used behind the Diffie Hellman key exchange protocol [4].

3.2 Domain Parameters

The set of parameters {*l*, *m*, *p*, *G*, *n*, *h*} are the domain parameters for Elliptic Curve Cryptography where *l* and *m* are the curve parameters; *p* is the prime number; *G* is a point on the curve that generates a cyclic subgroup; *n* is the order of the subgroup generated by the *G*; *h* is the cofactor. Ideally, *h*=1. The parameter n is the least positive integer such that $nG = \mathcal{O}$ (the point at infinity). The set of domain parameters is the information required by all the parties in order to implement protocol. [8].

3.3 Implementation

In this section, the implementation of Elliptic Curve Cryptosystem is discussed. All the parties which are communicating on a public network are aware of the domain parameters. In particular, if there are two parties then, both the parties choose their private keys say $\alpha, \beta \in Z$ respectively.

$$1 \leq \alpha \leq n-1$$

$$1 \leq \beta \leq n-1$$

Both parties evaluate the following points and send them publically to each other.

1^{st} party: $A = \alpha G$

2^{nd} party: $B = \beta G$

Despite of knowing the points A (x_A, y_A) and B (x_B, y_B), no one on the public network can find the values of scalars α and β. Using B and its private key α, the first party computes $\alpha B = \alpha\beta G$. Similarly, using A and its private key β, the second party computes $\beta A = \beta\alpha G$. As the scalar multiplication is commutative, they reach the same point without even knowing each other's secret keys [9].

IV. ECC vs RSA

Elliptic curve cryptography provides smaller key sizes as compared to RSA and other public key cryptography methods. Small key sizes require less storage memory, less power consumption and fewer processing units to

ISBN: 978-93-86171-33-7

implement the protocol. Smaller keys of ECC provide same level of security as compared to RSA. For example, 1024 bit security potency of RSA is similar to 163 bit security potency of ECC [10, 11]. Table 4.1 represents the key sizes for RSA and ECC with same security level [11-13].

Table 4.1 Comparison between RSA and ECC

Security Level (in Bits)	RSA: Modulus Size (in Bits)	ECC: Key Size (in Bits)	Key Size Ratio
80	1024	160	6.4:1
112	2048	224	≈9.1:1
128	3072	256	12:1
192	7680	384	20:1
256	15360	512	30:1

V. CONCLUSION

The remarkable applications of elliptic curves in secret writing make them significant for research. The operation of scalar multiplication in elliptic curves is considered to be more efficient computationally as compared to exponentiation in RSA. The advantage of ECC over RSA is that it maintains same level of security and provides faster communication using smaller key sizes. It has been incorporated in many security standards because of its efficient implementation. Moreover, ECC is quite appropriate for wireless communications, like mobile phones and smart cards. In order to enhance the security level of ECC, improvement can be made in scalar multiplication algorithm.

REFERENCES

[1] Nicholas G. McDonald, A research review: Past, Present and Future Methods of Cryptography and Data Encryption, University of Utah, 2009, 13-19.

[2] Gary C. Kessler, An Overview of Cryptography, 2010, 37-39. Available from: <http:www.garykessler.net/library/crypto.html>.

[3] S. Kaur, The Role of Mathematics in Emergence of Cryptography: A Review, International Journal of Advance Research in Science and Engineering, 6(1), 2017, 230-234.

[4] V. S. Miller, Use of Elliptic Curves in Cryptography, Conference on the Theory and Application of Cryptographic Techniques, Springer Berlin Heidelberg, 1985.

[5] D. Hankerson, A. Menezes, S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, NY, USA, 2004, 11-16.

[6] M. S. Anoop, Elliptic Curve Cryptography, An Implementation Guide, 2007.

[7] M. Joye, C. Tymen, Protections against Differential Analysis for Elliptic Curve Cryptography: An Algebraic Approach, Cryptographic Hardware and Embedded Systems, France, 2001, 377-390.

ISBN: 978-93-86171-33-7

[8] A. Cilardo, L. Coppolino, N. Mazzocca, L. Romano, Elliptic Curve Cryptography Engineering, Proc. 94th IEEE Conf., 2006, 395-406.

[9] Ian F. Blake, Gadiel Seroussi, Nigel P. Smart, Advances in elliptic curve cryptography, Cambridge University Press, 317, 2005.

[10] M. Savari, M. Montazerolzohour, Y. E. Thiam, Comparison of ECC and RSA Algorithm in Multipurpose Smart Card Application, International Conference on Cyber Security, Cyber Warfare and Digital Forensic, 2012, 49-53.

[11] M. Bafandehkar, S. Yasin, R. Mahmod, Z. M. Hanapi, Comparison of ECC and RSA Algorithm in Resource Constrained Devices, International Conference on IT Convergence and Security, 2013, 1-3.

[12] M. Prabu, R. Shanmugalakshmi, A Comparative and Overview Analysis of Elliptic Curve Cryptography over Finite Fields, International Conference on Information and Multimedia Technology, 2009, 495-499.

[13] M. J. B. Robshaw, Y. L. Yin, Elliptic Curve Cryptosystems, An RSA Laboratories Technical Note 1, 1997, 997.