International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 1, January 2013 ISSN 2319 - 4847

Prospective Utilization of Elliptic Curve Cryptography for Security Enhancement

Sonali Nimbhorkar[1], Dr.L.G.Malik[2]

[1] Research Scholar, Computer Science & Engineering
G.H.Raisoni College of Engineering, Nagpur, India

[2] Computer Science & Engineering
G.H.Raisoni College of Engineering, Nagpur, India

ABSTRACT

Now a days Elliptic curve cryptography (ECC) is the most efficient public key encryption scheme based on elliptic curve concepts that can be used to create faster, smaller, and efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the conventional method of key generation. This scheme can be used with public key encryption methods, such as RSA, and Diffie-Hellman key exchange. Digital Signature. This paper presents potential use of elliptic curve cryptography for communication network.

Keywords: Elliptic curve cryptography (ECC), coordinate system, scalar multiplication, level of security, Elliptic curve, finite field**.**

1. INTRODUCTION

Rapid development on electronic technology secure communication in particular is in demand for any kind of communication network .The main component of secure communications software stack includes key exchange and signatures which is required for public key algorithms like RSA,DSA and elliptic curve cryptography[4][6] .Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller. The discrete logarithm problem on elliptic curve groups is believed to be more difficult than the corresponding problem in the underlying finite field [13][14][15].Elliptic Curve Cryptography provides level of security with a 164-bit key that RSA require a 1,024-bit key to achieve, Because ECC helps to establish equivalent security with lower computing power and battery resource usage. The ECC covers all primitives of public key cryptography like digital signature ,key exchange, key transport ,key management .Presently ECC has been commercially adopted by many standardize organization such as NIST ,ISO ,and ANSI [1] .ECC covers the discipline of mathematics and computer science and engineering .It can widely used for electronic commerce , secure communication ,etc. The security of the Elliptic Curve Cryptography depends on the difficulty of finding the value of k, given kP where k is a large number and P is a random point on the elliptic curve[5][21]. This is the Elliptic Curve Discrete Logarithmic Problem. The elliptic curve parameters for cryptographic schemes should be carefully chosen in order to resist all known attacks of Elliptic Curve Discrete Logarithmic Problem (ECDLP)[21][23].

The rest of this paper is organized as follows: Section 2 describes definition of elliptic curves, and operations performed on elliptic curves ,Section 3 discusses the main security consideration for elliptic curve cryptography , comparison of ECC with RSA ,and section 4 analyze the implementation consideration of ECC for communication network ,elliptic curve applications is explained in section 5 .Finally ,conclusion is described in section 6.

2. CONDITIONS OF ELLIPTIC CURVES

2.1Definition of Elliptic Curve

Elliptic curves the name come from elliptic integral .Elliptic Curves have nothing to do with ellipses .Elliptic curves appear in many areas of mathematics varies from number theory to complex analysis and from cryptography to mathematical physics[14][15].The elliptic curves is a curve that also forms a groups. Group laws are constructed geometrically. Induction method is a tool of mathematical proof typically used to establish that a given statement is true for all natural numbers or not. The base behind to give the concepts elliptic curves formation is method of diophantus. Diophantus method is used to represent algebraic notation and symbols. Diophantus had given principle to convert any generalized equation to simpler form according requirement. Method of diophantus uses a known set of points to produce new points [3][4].Graphical representation of elliptic curve as follows[16][21]:

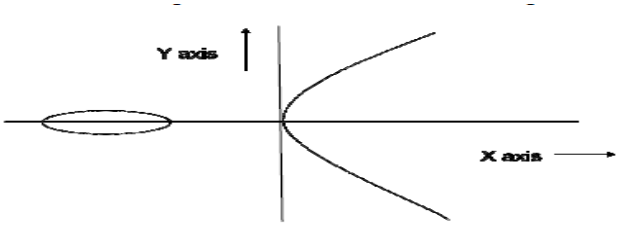

Figure 1. Graphical Representation Of Elliptic Curves

Curves of elliptic nature are called as elliptic curves. An elliptic curve over a field K is a nonsingular cubic curve in two variables, f(x, y)=0 with a point which may lie at infinity. The field K may be complex numbers ,real ,rational ,algebraic extensions or finite field. Field is a set of elements on which two arithmetic operation(addition ,multiplication). Use of elliptic curves groups over the finite field Fp or F_2^m[9].Speed and accuracy are important parameters for cryptography. In elliptic curve point arithmetic is the factor that decides the cost of point operation such as point addition ,point doubling and point tripling in elliptic curve cryptography[8].Therefore efficient implementation of point arithmetic is very important .The basic field arithmetic operations are addition ,subtraction, multiplication ,squaring and inversion can be separated into three distinct layers as follows[19][20]:

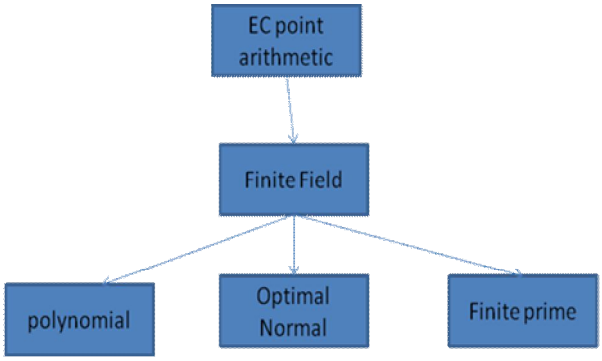

Figure 2. Scalar Point Calculation

2.2 Generalized form of Elliptic Curves

Generalized form of weierstrass equation of elliptic curves as given below [8][9][21][22]:

$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ ---------- (1)

Where a1,a2,a3,a4,a6 are real numbers belong to R, x and y take on values in the real numbers. If L is an extension field of real numbers, then the set of L-rational points on the elliptic curve E. (1) is called Weierstrass equation. For the purpose of the encryption and decryption using elliptic curve it is sufficient to consider the equation of the form $y^2 = x^3 + ax + b$. Here the elliptic curve E is defined over the field of integers K, because a1, a2, a3 , a4, a6 are integers. If E is defined over the field of integers K, then E is also defined over any extension field of K. Weierstrass equation of elliptic curve is the two variable equation forms a curve in the plane[8][9].

2.3 Techniques of scalar multiplication

The major cryptographic function in Elliptic Curve Cryptography is scalar point multiplication which computes Q = kP, a point P is multiplied by an integer k resulting in another point Q on the curve. Scalar multiplication is performed through a combination of point additions and point doublings, e.g. 11P = 2((2(2P)) + P) + P*[14][15][20][21][22].
Discrete methods to represent scalars are as follows:

2.3.1Single Scalar Multiplication:- Let E be an elliptic curve over a field K, P a point in the group E(K), a positive integer k [1, n - 1], where n is the order of E(K). Then the computation of [k]P is called single scalar multiplication.

2.32 Double Scalar Multiplication:- Let E be an elliptic curve over a field K, P and Q two distinct points in the group E(K), k. Two distinct positive integers in the interval [1, n - 1] where n is the group order of E(K). Then the computation of [k]P + [l]Q is called double scalar multiplication.

Scalar multiplication is the computationally heaviest operation in signature verification in elliptic curve based cryptosystem. The most important objective of scalar multiplication is to improve the speed of both types of scalar multiplication. in general ,there are several approaches to accomplish the purpose selection is discussed [4][9] that focuses on :

- Proper usage of coordinate systems.

- Selecting arithmetic efficient curves.
- Combination of operation, sometimes point addition and point multiplication performed together to reduce the number of field operation.
- Different representation for scalars**.**

For the implementation of scalar multiplication following forms are used such as Right-to-left binary method, Left-to-right binary method, Non Adjacent Form, Width -w Nonadjacent Form Joint Sparse Form ,Double and add form ,Addition chains ,Fibonacci and add ,Montgomery method .
Implementation of point multiplication can be separated into three distinct layers like Finite field arithmetic, Elliptic curve point addition and doubling, Point multiplication scheme makes secure against attacks, various methods have been suggested using special point representations for specifically chosen elliptic curves[23] recommended by NIST and SECG. Also provides efficiency advantages over earlier proposals.

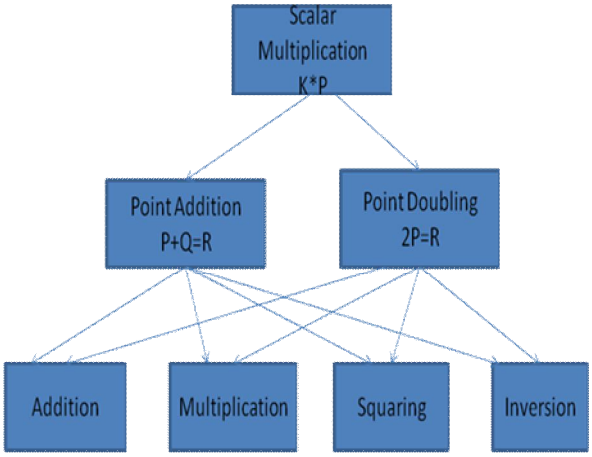

Figure 3. Hierarchy of scalar Multiplication.

2.4 Preferences for Coordinate Systems

Point additions(PA) and point doublings(PD) can be implemented using coordinate system [10][11]like Affine coordinate system, Standard projective ,Standard projective and affine ,Jacobian projective ,Jacobian projective and affine, Lopez –Dahab .
The most popular coordinate representation is affine representation which is based on two coordinate (x,y) and other representation such as projective ,jacobian , lopez-dahab uses three coordinates .Transforming affine coordinates into one of the other representation is almost simple but not vice versa, since transformation requires costlier field inversion[12][13].

3. ELLIPTIC CURVE CRYPTOSYSTEM

Elliptic curve cryptography (ECC) is a public-key cryptosystem like RSA, Rabin, and El-Gamal encryption algorithm. Every user has a public and a private key. Public key is used for encryption and signature verification. Private key is used for decryption and signature generation. Elliptic curves are used as an extension to other current cryptosystems such as Elliptic Curve Diffie-Hellman Key Exchange, Elliptic Curve Digital Signature Algorithm. The central part of any cryptosystem involves elliptic group [10][13][14][15] .
The Formal methodology of Elliptic Curve Cryptosystem for operation on E is as follows:

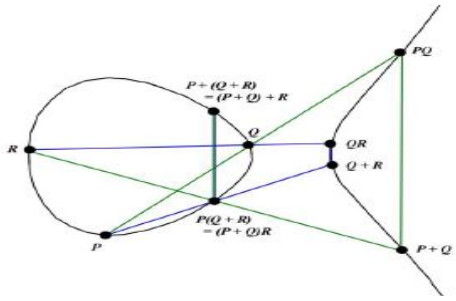

Figure 4. Associativity of Group Laws on Curves.

The points on the elliptic curve form an addition group, an Abel group. The addition rule of two points is explained in the following ways. There are two cases one is two points are distinct and second is two points are same.

Suppose two points P and Q are on the elliptic curve and P is not equal to Q, first draw a line passes these two points, then compute the intersection point T of the line and the curve, after this, draw a line passing point T, which is paralleling Y coordinate, finally compute the intersection point R of the line and the curve, and point R is the result, that is to say, R = P+Q. If P is equal to Q, then, draw a tangent line of the curve at point P, and compute the intersection point T of the line and the curve, draw a line passing point T, which is paralleling Y coordinate, finally, compute the intersection point R of this line and the curve and point R is the result that is R = 2P[21][22].
For associativity, it must show that if P, Q, and R are arbitrary points in E, then (P+Q)+R=P+(Q+R). Consider the following lines involved in the step-by-step construction of (P+Q)+R, and P +(Q+R). The third point listed will always be the residual third point in E on the line specified by the first two points given in E[22].

3.1 Security Consideration

Security is the most attractive feature of elliptic curve cryptography. Elliptic curve cryptosystems also are more computationally efficient than the first generation public key systems like RSA, DSA and Diffie-Hellman key exchange algorithm. Table1 gives approximate equivalent key sizes for ECC and RSA algorithm. From the table 1 it is clear to see that ECC affords the same security as RSA while using significantly smaller key sizes. In Table 1, at all levels of security including 512 bits, ECC has smaller public key sizes than both RSA and DSA/DH. Because of its smaller key size, ECC outperforms both RSA and DSA/DH for most routine operations while offering comparable levels of security. The reason is that ECC provides greater efficiency in terms of computational overheads, key sizes and bandwidth. In implementations, these savings mean higher speeds, lower power consumption .For efficient cryptosystem implementation ANSI(American national standard institute)and NIST(national Institute of standard and technology)are producing standards and technology[13][14] .

Table 1. Key Size Strength (Suggested by NIST)

Time to break in MIPS years	RSA/DSA key size	ECC key size	RSA/ECC Key size ratio
10^4	512	106	5:1
10^8	768	132	6:1
10^{11}	1024	163	7:1
10^{20}	2043	210	10:1
10^{78}	21000	600	35:1

4. PERFORMANCE PARAMETERS FOR ELLIPTIC CURVE CRYPTOGRAPHY IMPLEMENTATION

Although RSA ,El-GAMAL and Diffie –Hellman are secure asymmetric key cryptosystem, their security comes with a price ,their large keys. So researchers have looked for providing substitute that provides the same level of security with smaller keys. For Elliptic Curve Cryptography implementation following consideration should meet [1][2][4][9] :

- Suitability of methods available for optimizing finite field arithmetic like addition, multiplication, squaring, and inversion.
- Suitability of methods available for optimizing elliptic curve arithmetic like point addition, point doubling, and scalar multiplication.
- Application platform like software, hardware, or firmware.
- Constraints of a particular computing environment e.g., processor speed, storage, code size, gate count, power consumption.
- Constraints of a particular communications environment e.g., bandwidth, response time.

Efficiency of ECC is depends upon factors such as computational overheads ,key size, bandwidth ,ECC provides higher-strength per- bit which include higher speeds, lower power consumption, bandwidth savings, storage efficiencies, and smaller certificates.

5. APPLICATION OF ELLIPTIC CURVE CRYPTOGRAPHY

Many devices are constrained devices that have small and limited storage and computational power, for constrained devices ECC can be applied [16][17][23].

- For wireless communication devices like PDA's multimedia cellular phones ECC can apply.
- It can be used for security of Smart cards, wireless sensor networks, wireless mesh Networks.
- Web servers that need to handle many encryption sessions.
- Any kind application where security is needed for our current cryptosystems.

6. CONCLUSION

Elliptic Curve Cryptography offers the highest strength-per-key-bit of any known public-key system of first generation techniques like RSA, Diffie-Hellman. ECC offers the same level of security with smaller key sizes, computational power is high. Integrated circuit space is limited for smart card, wireless devices. The ongoing development of standards is a very important position for the use of a cryptosystem. Standards help to ensure security and interoperability of different implementations of one cryptosystem. There are several major organizations that develop standards like International Standards Organization (ISO), American National Standards Institute (ANSI), Institute of Electrical and Electronics Engineers (IEEE), Federal Information Processing Standards (FIPS).The most important for security in information technology are the in addition secure communication, Elliptic curve cryptography (ECC) enabling technology for numerous wireless sensor networks.

REFERENCES

[1] Andrej Dujella "Applications of elliptic curves in public key cryptography" Basque Center for Applied Mathematics and Universidad del Pais Vasco / Euskal HerrikoUnibertsitatea, Bilbao, May 2011.

[2] Pardeep Malik "Elliptic Curve Cryptography For Security Inwireless Networks" Statistics 2011 Canada: 5th Canadian Conference in Applied Statistics/ 20th conference of the Forum for Interdisciplinary Mathematics - Interdisciplinary Mathematical Statistical Techniques, July 1-4-2011, Concordia University, Montreal, Quebec, Canada.

[3] Michael Naehrig "Pairings on elliptic curves – parameter selection and efficient computation", Workshop on Elliptic Curve Computation ,Redmond, 19 October 2010

[4] Dr.R.Shanmugalakshmi, M.Prabu" Research Issues on Elliptic Curve Cryptography and Its applications "IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009.

[5] Mathias Schmalisch, Dirk Timmermann "Comparison of Algorithms for Finite Fields of GF(2m)",The IASTED International Conference on Communication, Network, and Information Security.CNIS 2003, December 10-12, 2003New york,USA.

[6] F.Amin ,A.H.Jahngir and H.Rasifard "Analysis of Public –Key Cryptography For Wireless Sensor Networks Security" World Academy Of Science ,Engineering And Technoly41 2008.

[7] R. Rajaram Ramasamy and M. Amutha Prabakar "Digital Signature Scheme with Message Recovery Using Knapsack-based ECC" International Journal of Network Security, Vol.12, No.1, PP.12,7, Jan. 2011

[8] Vassil Dimitrov, Laurent Imbert, And Pradeep K. Mishra "The Double-Base Number System And Its Application To Elliptic Curve Cryptography"MATHEMATICS OF COMPUTATIONS 0025-5718(07)02048-0,Article electronically published on December 11, 2007.

[9] LIU Shuanggen,LI Ping,HU Yupu "Improvement Schemes for Scalar Multiplication Algorithm in Elliptic Curve Cryptography" ISSN:1000-3428.0.2006-17-009

[10] Mrs. Megha Kolhekar "Implementation Of Elliptic Curve Cryptography On Text. And Image"International Journal of Enterprise Computing and Business SystemsISSN (Online) : 2230 2230-8849Vol. 1 Issue 2 July 2011.

[11] Sergey Morozov,Christian Tergino,Patrick Schaumont "System Integration of Elliptic Curve Cryptography on an OMAP Platform" 2011 IEEE.

[12] Xiaojiang Du, Mohsen Guizani, Yang Xiao Hsiao-Hwa Chen "A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks", 2009IEEE.

[13]www.certicom.com

[14]William stallings "cryptography and network security principles and practice"fifth edition ,pearson ,2011.

[15]Behrouz A Forouzan,Debdeep Mukhopadhyay "cryptography and network security "second edition.Mc-Graw Hill.2008.

[16]Tingdingchen,Huiyun Li,Keke Wu,Fengqi Yu "Evaluation criterion of side channel countermeasures for elliptic cryptography devices" DOI10.1109/ICCCS.2009.13.

[17]Xue Sun,Mingping Xia "An improved proxy signature based on elliptic curve cryptography" DOI10.1109/ICCCS.2009.36.

[18]yinggjie Qu,Zhengming Hu "Research And Design Of Elliptic Curve Cryptography"978-1-4244-5824,-0,2010IEEE
[19]V.Gayoso Martinez,F.Hernanddez,L.Encinas,C.Sanchez Avila "A Comparioson Of The Standardized Versions Of ECIES, 978-1-4244-7409-7,2010IEEE.
[20]Abdahossein rezai,parviz kashvarzi "high perfomance implemetation approach of elliptic curve cryptosystem for wireless network applications,978-1-61284-459-6/11,IEEE 2011.
[21]Moncef Amara,Amar Siad"Elliptic Curve Cryptography And Its Applications" 2011 7th international workshop on systems ,signal processing and their applications(WOSSPA)
[22] Guicheng Shen ,Bingwu Liu "Research on Efficiency of computing kP in Elliptic Curve System" .,supported by funding project for science and technology program Beijing,2010 under grant numberKM20101010037002.
[23] Sonali U Nimbhorkar, Dr.L.G.Malik" A Survey On Elliptic Curve Cryptography (Ecc)" International Journal of Advanced Studies in Computers, Science and Engineering(IJASCSE), vol 1 issue1 ISSN 2278-7917 ,5 july2012.

AUTHOR

Sonali U Nimbhorkar received Post Graduate degree in computer science from RTMNU, Nagpur . she has published more than 19 research papers in various international journals and international conferences as an main author and co-author in the field of issues related wireless network ,wireless mesh network, network security and cryptography . At present she is assistant Professor in Computer Science & engineering Department in G.H.Raisoni College of Engineering Nagpur, India.