ISSN No. 0976-5697

Volume 4, No. 6, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

Implementation of Elliptic Curve Cryptography in Primary Field

Miss. Namrata Sable*, Mr. Avinash P. Wadhe
Department of Computer Science & Engineering,
G. H. Raisoni College of Engineering and Management, Amravati.
namratasable10@gmail.com*, aviwadhe@gmail.com

Abstract: Elliptic Curve Cryptography (ECC) is emerging as an attractive alternative to traditional public-key cryptosys- tems (RSA, DSA, DH). ECC offers equivalent security with smaller key sizes resulting in faster computations, lower power consumption, as well as memory and bandwidth sav- ings. While these characteristics make ECC especially ap- pealing for mobile devices, they can also alleviate the com- putational burden on secure web servers.

Keywords: Networks; security; key Management, ECC, Diffie–Hellman.

I. INTRODUCTION

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. 'Domain parameters' in ECC is an example of such constants. Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but it is much slower than the private key cryptography. The mathematical operations of ECC is defined over the elliptic curve y 2= x3+ ax + b, where 4a3 + 27b2 ≠0. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.

II. RELETED WORK

Wireless mesh network is a multihop communication .All packet generate from source to target node in hop by hop forwarding manner .To ensure the authenticity of each node is very much essential and communication must be secure. There is reach literature available on key management and intrusion detection method which discussed about secure communication in multihop wireless mesh network .In Farad T. Bin Muhaya, Fazl-e-Hadi, AtifNaseer[1] worked on selfish node detection in WMN by focusing routing information. Every node calculates field value from their neighbors .Every node has the information about neighbor's field values sefish node. Every node calculates its field value from their neighbors every node in the network has the information about their neighbor's field value. The node always forwards the packet having highest field value and hence the packet reaches to its destination. But not talk about scalable key management and proper authentication.

M.Imani, M.E.Rajabi, M. Taheri, M.Naderi [5] proposed the Vulnerabilities in network layer at wireless mesh network gives the survey on The various Vulnerabilities are: Selective forwarding and Blackhole attack, Sinkhole attack, Sybil attack, Wormhole attack, Rushing attack. As all of the wireless networks suffer from many vulnerabilities and conclude that The efficient method for preventing external attacker is cryptography with a globally shared key needed.

ZHAI Min, HUANG Ting-Ieicode [5] proposed Public key infrastructure and Certificate authority (CA) which are two very important authentication mechanisms. Because the wireless mesh network does not have pre established trusted network architecture, therefore, it is unrealistic to establish a central centralized CA. Problem encountered when the service node changes then information required re-distributed and old node will be a security risk. However, it is not easy for off-line CA to frequently re-distribute all the sub-secret of services nodes on account of heavy workload. Need proper and efficient protocol for authentication.

Andreas Noack, Jorg Schwenk [7] proposed the application of group key agreement (GKA) protocols. They compare the performance of three group key agreement protocols in new model: Burmester-Desmedt I (BD1), Burmester-Desmedt II (BD2) and the Tree Based Key Agreement (TBKA) protocol. All of the chosen protocols support any positive number of mesh nodes greater than one. Under a cryptographic perspective, there are some slight differences in the security properties of the mentioned protocols but fail to give scalable key management.

© 2010, IJARCS All Rights Reserved

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

III. METHODOLOGY

A. *ECC Public Key Kryptosystem:*

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each node are taking part in the communication. Mostly have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Private key is known to only device themselves whereas the public key is known to every device in communication. In mostly public key algorithm require a set of predefined parameter to be known by all the communicating parties. 'Domain parameters' in ECC is an example of such parametric cryptography.

ECC has emerging as powerful the security solutions for wireless networks due to the small key size and low computational overhead. For example, 160- bit ECC offers the comparable security to 1024-bit RSA. An elliptic curve over a finite field GF (a Galois Field of order q) is composed of a finite group of points (xi, yi), where integer coordinates xi, yi satisfy the long Weierstrass form:

$$y2 + a1xy + a3y = x3 + a2x2 + a4x + a6$$

B. *ECC-based access control:*

An elliptic curve consists of the points satisfying the equation:

$y^2=x^3$+ax +b

Where x, y, a and b are elements in GF (q) (a *Galois Field* of order, where is q a prime).

Each choice of (a, b) yields a different elliptic curve. Lets take example, Figure 2 shows an elliptic curve of

$y^2 = x^3$+7x

Therefore (a,b) are (7,0) and lets take any two point such as

P (-2.35,-186)
Q (-0.1, 0.836)

so that line can be drawn through both point and intersect to curve and we get point R on the curve that explain below in figure 1.

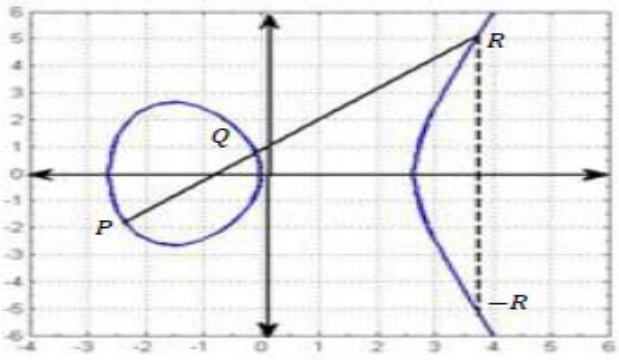

Figure: 1

$y^2 = x^3$+7x
P+Q=R= (3.89,-5.62)
-R (3.89,-5.62)

Figure 1: Elliptic Curve and Point Addition [18]

The elliptic curve group operation is closed under addition so that addition of any two points is also a point in the group. Given two points P (x_1, y_1) and Q (x_2, y_2) , the addition results in a point R (x_3, y_3) given by:

$(x_1, y_1)+(x_2, y_2)=(x_3, y_3)$

such that

x_3= β2+ β+x_1+x_2+a

y_3=β (x_1+x_3) + x_3+y_1

β = (y_1+y_2) / (x_1 + x_2) (slope of line)

An example of P (-2.35,-186) and Q (-0.1, 0.836) is illustrated in Figure 1.

If P=Q, then R = P+P=2P. Addition of multiple points will give. ECC is strong for attach due to difficulty of the Elliptic Curve Discrete Logarithm Problem , that is, given points P and Q of the group, it is practically infeasible to find a number K such as .Q=k × P.

C. *Elliptic Curve Diffie-Hellman Protocol (ECDH):*

Elliptic Curve Diffie-Hellman (ECDH) protocol is a secret key exchanging protocol to establish a secret key between two parties who have no prior knowledge about each other. Based on ECDLP,[19] a typical ECDH is built as shown in Figure 3. Initially, Alice and Bob agree on system based point P and generate their own pair key (Q_A, K_A) and (Q_B,K_B) .To share a secret, Alice and Bob exchange their public keys, and then use their own private key, K_A and K_B respectively. To multiply the other's public key, i.e. The original Diffie-Hellman secret sharing protocol (Diffie and Hellman, 1976) requires a key of at least 1024 bits to achieve sufficient security. Unfortunately, low-power architecture, such as MSP430 andATMega128, cannot afford the large memory overhead. Diffie–Hellman scheme based on ECC, however, can achieve the same security level with only 160 bit key size. A typical Elliptic Curve Diffie–Hellman (ECDH) scheme is shown in Figure 2. Initially, Alice and Bob agree on system base point P and generate their own public key QA and QB. To share a secret, Alice and Bob exchange their public keys and then use their own private key to multiply the other's public key. The result point R will be the secret. Eve, an eavesdropper, may overhear the communication and learn the public keys from Alice and Bob. However, with the knowledge of PQA and QB, it is computationally intractable for Eve to get Alice and Bob's private keys. As a result, she cannot figure out secret R.

An example of ECC version of Diffie-Hellman

Private Key K_A	⟶	Private key K_B
R=K_A × Q_B	⟵	R = K_B × Q_A
Compute secret	Q_B= K_B ×P	Compute Secret
Alice	Q_A = K_A×P	**Bob**

Figure 2: ECDH Key Exchange Protocol

D. *Elliptical curve Over Finite Field:*

ECC make use of elliptic curve in which variables and coefficient all are restricted to element of finite field. Two families of elliptic curve are used in cryptographic

© 2010, IJARCS All Rights Reserved

applications: For prime curve over Z_p and for binary curve over GF(2^m) .poions out that prime cur are best for software applications because the extended bit-fiddling binary operations needed by binary curves are not required; and that binary curve are best for hardware applications. In this paper we focused on primary field operations.

Elliptic curves over GF(p) are of the form

y2 (mod p)= x3+ax+b mod p

For a,b values in equation can be verified by calculating $(4a^3+27b^2)$mod p$\neq$.0 for specific values of a and b. for satisfying geometric terms. All operations values such as required addition, subtraction, division, multiplication involves integers between 0 to p-1.so that relative public and private can easily generated for sustain security.

Prime p is chosen such that there is finitely large number of points on the elliptic curve to make cryptosystem secure. The multiplication of points by a scalar is a series of additions and doubling of points. That is, we define ***kP***, where ***k*** an integer and ***P*** is a point , by repeated addition in the natural manner. The value of *kP* may be efficiently computed via repeated doubling . That is,vthe refected point multiplication converts P to –P by negating the y coordinate of P i,e the negative of P=(x,y) gives –P=(x,-y).

E. Calculating Point On The Curve:

The following algorithm in figure 4 gives the points on the curve Ep(a,b).

Algorithm Finding Elliptic_Points(p,a,b)

1. Initilize variable x =0 .
2. Begin
3. Claculate the value of (x3+ax+b) mod p and stored it in z.
4. And check vale of z also , is perfect square in Zp.
5. If z is perfect squre then Go to step 6.
6. R(x,sqrt(z), y,sqrt(z)).
7. Increment value of x by one
8. until x is smaller than p
9. STOP

Figure. 3 Algorithm For Elliptical Curve Point

IV. CONCLUSION AND FUTURE WORK

ECC has attracted much attention as the security solution for wireless networks due to the small key size and lowcomputational overhead. For example 160-Bit ECC. Offers the comparable security to 1024-bit RSA. Implementation of ECC on primary field performance will increase substancially; in future it is possible to further reduce the running time by using more refined and careful programming

V. REFERENCES

[1] Fahad T. Bin Muhaya, King Saud University Fazl-e-Hadi AtifNaseer (2010), "Selfish Node Detection in Wireless Mesh Networks" . 201O International on Networking and Information Technology.

[2] Yatao Yang Ping Zeng Xinghua Yang Yina Huang (2010),"Efficient Intrusion Detection System Model in Wireless Mesh Network" Second International Conference on Networks Security, Wireless Communications and Trusted Computing

[3] Jinyuan Sun, Chi Zhang (2011), "SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks" ieee transactions on dependable and secure computing, vol. 8, no. 2,

[4] ZHAI Min, HUANG Ting-Iei (2010), "A RSA Keys harinScheme based on Dynamic Threshold Secret Sharing Algorithm for WMNs". 978-1-4244-6837 9/10/$26.00 ©2010 IEEE

[5] M.Imani Bing He, S M.E.Rajabi M.Naderi (2010) "Vulnerabilities in network layer at Wireless Mesh Networks (WMNs) ".International Conference on Educational and Network Technology (ICENT 2010)

[6] Bing He, Saugat Joshi, Dharma P. Agrawal (2010), "Group Key Agreement Performance in Wireless Mesh Networks". 35th Annual IEEE Conference on Local Computer Networks LCN 2010, Denver, Colorado

[7] Andreas Noack J¨org Schwenk (2010), "Group Key Agreement Performance in Wireless Mesh Networks" 35th Annual IEEE Conference on Local Computer Networks

[8] Vipul Gupta, Douglas Stebila_, Stephen Fung Eberle "Speeding up Secure Web Transactions Using Elliptic Curve Cryptography"Sun Microsystems, Inc.2600 Casey Avenue Mountain View, CA 94043

[9] ANSI X9.63 (1999.), "Elliptic Curve Key Agreement and Key Transport Protocols", American Bankers

[10] Li, X. Xin and Y. Hu, (2007) "Key management in ad hoc networks using self-certified public key system", International Journal of Mobile Communications, vol. 5(1), pp. 94-106.

[11] S Mittra, "Iolus (1997,) a framework for scalable secure multicasting," in Proceedings of ACM SIGCOMM'97, Canada, September, pp.14-18.

[12] F Lee and S. Shieh, (2004) "Scalable and Lightweight Key Distribution for Secure Group Communications," International Journal of Network Management, 14:167-176.

[13] Y. Fu, J. He, R. Wang and G. Li, (2004) "A key-chain-based keying scheme for many-to-many secure group Communication," ACM Transactions on Information and System Security (TISSEC), vol. 7(4), pp. 523 – 552.

[14] M S. Siddiqui, and C. S. Hong, (2007) "Security Issues in Wireless Mesh Networks", Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE'07). New York IEEE Press, pp. 41−47.

[15] H. Mu and Y. Liu, (2006) "Mesh Based Multicast Key Management Scheme in Ad Hoc Networks," in Proceedings of IEEE ICSP, pp.

© 2010, IJARCS All Rights Reserved

[16] Patrick Longa, and Catherine Gebotys, "Efficient Techniques for High-Speed EllipticCurveCryptography" 2010 University of Waterloo, Canada

[17] Kossi Edoh"Elliptic Curve Cryptography on PocketPCs*" International Journal of Security and Its Applications Vol. 3, No. 3, July, 2009

[18] Darrel Hankerson, Julio Lopez Hernandez, Alfred Menezes, Software Implementation of" Elliptic Curve Cryptography over Binary Fields", 2000, Available at

[19] http://citeseer.ist.psu.edu/hankerson00software.html

[20] http://scribed.com/enhance/ network security-using- ecc

[21] E-book -Cryptography and Network Security by William Stalling

[22] E-book-Advances In Elliptic curve cryptography by londan mathematical society.

Short Bio Data for the Author

 **Prof. Avinash P. Wadhe**: Received the B.E from SGBAU Amravati University and M-Tech (CSE) From G.H Raisoni College of Engineering, Nagpur (an Autonomous Institute). He is currently an Assistant Professor with the G.H Raisoni College of Engineering and Management, Amravati SGBAU Amravati University. His research interest include Network Security, Data mining and Fuzzy system .He has contributed to more than 20 research paper. He had awarded with young investigator award in international conference.

 Namrata Sable received the B.E. from RTMNU, Nagpur university and pursuing ME(CSE) from G. H. Raisoni College Of Engineering & Management, Amravati. Her Research interest include Network Security, Data mining and Fuzzy system .He has contributed to more than 20 research paper. He had awarded with young investigator award in international conference.

© 2010, IJARCS All Rights Reserved