Vol1 No 1
Year 2019
Australian Journal of Wireless Technologies, Mobility & Security ISSN2200-1883

Implementation of Digital Signature Algorithm by using Elliptical Curve p-192

Darshana Pritam Shah[1],Namita Pritam Shah[2]
RV College of Engineering Bangalore India[1,2]

Abstract- The public key cryptographic algorithms considered unsuitable for Internet of Things due to use of longer keys, stressful calculations and consumption of battery resources for 16bit processers. This paper presents a novel algorithm based on elliptical curve for securing communication between internet of things by use of single coordinate system of Elliptical curve cryptography. Though lengdre symbol or single coordinate system exist in mathematics literature, it's use for securing IoT devices is fairly new. In the proposed system IoT device transfer one coordinate of public key with extra bit allowing to save 50 % of bandwidth and storage for IoT devices.

Key Terms: Elliptical Curve, Internet of Things, affine coordinate, projective coordinates, bandwidth etc

I INTRODUCTION

Internet of Things are gaining popularity day by day and will used extensively in all daily life applications in health, smart cities, military use, and airports and public places[1-5]. Once the 'Things' will become online , they will be susceptible to active and passive attacks from hackers. But due to resource constrained nature, providing security to these smaller devices having 16 bit controllers with limited memory and bandwidth will become tough task.

Most of the public key algorithms provide encryption, decryption and signature facilities like RSA, ECC[6-10]. On the other hand Diffie Hellman kind of algorithms are used for key pair establishment and the session key agreed by this algorithm is used for subsequent encryption and decryption.

However, this paper will concentrate on use of Elliptical curve due to its shorter key length for securing IoT device communication. In IoT environment, there are always constraints on memory and transmission power and bandwidth.

In this paper, we have presented mathematical proof and practical implementation of exchange of elliptical keys with single coordinates. An effective and efficient system was designed for the same purpose and tested on MIRACL crypto library. The program coding has been done in C language. The result windows are included in the paper for reader's convenience.

II ECDSA PROTOCOL

An elliptical curve with a prime field is represented by equation, $E: y^2 = x^3 + ax + b \ mod \ p$.
In our example we will take $E(f7): y^2 = x^3 + x + 3$.
There are six point as shown in Table 1 along with the point at infinity which satisfy equation $E: y^2 = x^3 + ax + b \ mod \ p$.These six points with point at infinity forms a finite close cyclic abelian group.

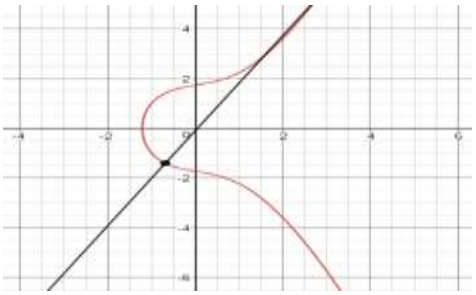

Fig 1. Elliptic curve $y^2 = x^3 + x + 3$

+	0	(4,1)	(6,6)	(5,0)	(6,1)	(4,6)
0	0	(4,1)	(6,6)	(5,0)	(6,1)	(4,6)
(4,1)	(4,1)	(6,6)	(5,0)	(6,1)	(4,6)	0
(6,6)	(6,6)	(5,0)	(6,1)		0	(5,0)
(5,0)	(5,0)	(6,1)	(4,6)	0	(5,0)	(6,6)
(6,1)	(6,1)	(4,6)	0	(5,0)	(6,6)	(5,0)
(4,6)	(4,6)	0	(5,0)	(6,6)	(5,0)	(6,1)

Table 1. Point on elliptic curve $y^2 = x^3 + x + 3$

The Table 1 shows that any operation performed on these points reults on a point on the the same curve. For example, if you will add (4,1) and (6,1) , the addition will be the point (4,6) which is the point on same curve.

Fig 1 sows the elliptical curve .Also if we assume that point P is (5,0) . Then we have [2] P = (6,1) ; [3]P =(4,6) ;[4] P = (0) ;[5]P =(5,0) ; [6]P=(6,6). So we have seen in this example E(F7) is a finite cyclic group of order six generated by point P.

An elliptical curve represented by an equation$(f7)$: $y^2 = x^3 + x + 3$, there are at the most two points on the elliptic curve with the same x coordinate. Table 1 shows that point (4,1) and (4,6) are having the same x coordinate. Thus we can conclude that any point p on the elliptical curve can be represented by its x-coordinate along with a bit b resulting in the saving of half of the point. A bit b is used to distinguish between two possibilities of the y coordinate as elliptic equation is quadratic equation and has two square roots. We can set b=0 if y <p/2 and or b=1 otherwise. This process is called as point compression. The author of this paper strongly recommends the point compression scheme while implementing elliptical curve cryptography for the resource constraint wireless sensor networks. The elliptical curve considered in this paper are of prime field. Mathematical treatment of binary field curve is beyond the scope of this paper.

III Implementation on MIRAXCL crypto library of proposed method

We have implemented Elliptic Curve Digital Signature Algorithm (ECDSA) with the proposed scheme of single coordinate [11-15]. The ECDSA program generates one set of public and private keys in files public.ecs and private.ecs respectively. Notice that the public key is almost 50 % shorter than the conventional key by use of single coordinate scheme. The curve y^2=x^3+Ax+b mod p parameter used in this case are as per below- (information {p,A,B,q,x,y}, where A and B are curve constant, G(x,y) is the point on the curve with order q. And p is prime modulus. The elliptical curve p-192 used for experimentation in this paper [3,4]

Curve P-192

p=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFFFFFFFFFF

A=-3

b=64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1

Q=FFFFFFFFFFFFFFFFFFFFFFFF99DEF836146BC9B1B4D22831

Gx=188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF1012

Gy=07192B95FFC8DA78631011ED6B24CDD573F977A11E794811

Seed d given 12345

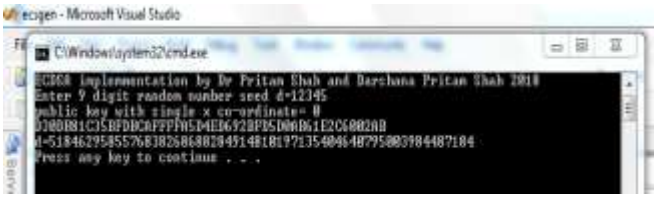

Fig 2 X coordinate with bit b =0

Seed d given is 1234567

Fif.3 X coordinate with bit b =1

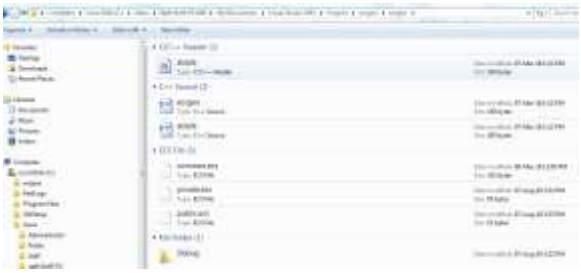

Fig.4Public and private keys generated

Fig. 5 Public key with bit b =1 and x coordinate

Fig.6 Public key with bit b =0 and x coordinate

IV Summary

The use of only one coordinate of public key of elliptical curve along with one extra bit will help IoT devices to save the bandwidth as well storage requirements. The IoT device overheads will be reduced by almost 50% as the key size reduced to half by use of only one coordinate. The mathematically it will also proved that at the receiver side if you have one coordinate and one extra bit, you can calculate the other coordinate. Due to its quadratic nature elliptical equation will have two solutions, one extra bit will help to differentiate between these two and to select the correct one.

V REFERENCES

1. Alzahrani, S.M. *Sensing for the Internet of Things and Its Applications*. in *2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. 2017.
2. Hu, F., D. Xie, and S. Shen. *On the Application of the Internet of Things in the Field of Medical and Health Care*. in *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*. 2013.
3. Kua, J., et al., *Using Active Queue Management to Assist IoT Application Flows in Home Broadband Networks.* IEEE Internet of Things Journal, 2017. **4**(5): p. 1399-1407.
4. Kunkun, P. and L. Xiangong. *Reliability Evaluation of Coal Mine Internet of Things*. in *2014 International Conference on Identification, Information and Knowledge in the Internet of Things*. 2014.
5. Lin, N. and W. Shi. *The research on Internet of things application architecture based on web*. in *2014 IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA)*. 2014.
6. Fang, X. and Y. Wu. *Investigation into the elliptic curve cryptography*. in *2017 3rd International Conference on Information Management (ICIM)*. 2017.
7. Qing-Hai, B., et al. *Research on Design Principles of Elliptic Curve Public Key Cryptography and Its Implementation*. in *2012 International Conference on Computer Science and Service System*. 2012.
8. Shah, D.P. and P.G. Shah. *Revisting of elliptical curve cryptography for securing Internet of Things (IOT)*. in *2018 Advances in Science and Engineering Technology International Conferences (ASET)*. 2018.
9. Shah, P.G., X. Huang, and D. Sharma. *Analytical Study of Implementation Issues of Elliptical Curve Cryptography for Wireless Sensor networks*. in *2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops*. 2010.
10. Shaikh, J.R., et al. *Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained E-commerce applications*. in *2017 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS)*. 2017.
11. Azaim, M.H., D.W. Sudiharto, and E.M. Jadied. *Design and implementation of encrypted SMS on Android smartphone combining ECDSA - ECDH and AES*. in *2016 Asia Pacific Conference on Multimedia and Broadcasting (APMediaCast)*. 2016.

12. Doerner, J., et al. *Secure Two-party Threshold ECDSA from ECDSA Assumptions*. in *2018 IEEE Symposium on Security and Privacy (SP)*. 2018.
13. Kodali, R.K. *Implementation of ECDSA in WSN*. in *2013 International Conference on Control Communication and Computing (ICCC)*. 2013.
14. Li, H., et al. *A Novel Algorithm for Scalar Multiplication in ECDSA*. in *2013 International Conference on Computational and Information Sciences*. 2013.
15. Zhang, C., L. Chi, and Y. Zhang. *Secure and Efficient Generalized Signcryption Scheme Based on a Short ECDSA*. in *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. 2010.