Comparatively Study of ECC and Jacobian Elliptic Curve Cryptography

Anagha P. Zele[1], Avinash P. Wadhe[2]

[1]Student of Master of Engineering (Computer Science & Engineering), Raisoni College of Engineering and Management, Amravati, India

[2]Assistant Professor, Computer Science & Engineering, Raisoni College of Engineering and Management, Amravati, India

Abstract: ***Elliptic curves were first proposed as a basis for public key cryptography in the mid-1980s independently by Koblitz and Miller. Elliptic curve cryptography (ECC) algorithm is practical than existing security algorithms. Because of this fact, it showed real attraction to portable devices (handheld devices) manufacturers and the security of their systems. In fact, through these devices, anyone can access either email, or do bank transaction or buy anything on internet using credit cards with high security standards. Elliptic curve algorithm is promising to be the best choice of these handhelds or similar devices because of low computing power and fast execution. ECC further gives very high security as compared to similar crypto systems with less size of key. For example, 160 bit ECC system is believed to provide same level of security as 1024 bit RSA [5, 6].The other two ECC scalar multiplication modular operations are inversion and multiplication. Inversion is known to be the complex and very expensive operation [7], its cost is reduced by converting the normal (x, y) affine coordinate system to projective coordinate system(X, Y, Z) which will add-up more modular multiplications to the process; i.e. it will increase the number of multiplications in both ECC point doubling and adding processes operations to reduce the inversion complexity.***

Keywords: ECC, JECC, public key cryptography, finite prime

1. Introduction

Elliptic Curve Cryptography is proposed independently by Neal Koblitz of the University of Washington and victor Miller of IBM in 1985. Elliptic curve cryptography is the public key cryptography .In Public key cryptography user and devices are take part in communication generally have two types of keys are public key and private key and set of operations associate with the elliptic curve cryptography[5] .In elliptic curve cryptography the key size is small hence it attract the much attention for security purpose[1].Elliptic curve cryptography gives very high security as compared to other cryptography with small size of keys.[1]For example 160 bit ECC is providing same level of security as 1024 bit RSA [1]. Elliptic curve cryptography is lower power consumption, faster computation and small bandwidth [2]. Elliptic curve cryptography is based on the coordinate system such as affine, projective, Jacobean, Chudnovsky-Jacobian and modified Jacobean coordinate systems [2]. ECC operations are usually done by using the affine coordinate[X, Y] [6]. ECC that uses the affine point it take long time for inversion it affects to the performance of ECC .researcher found some algorithm or methods to address the operation of inversion such as the Extended Binary GCD algorithm, and modular multiplication which were based on the Montgomery's method but this methods were costly in terms of time and resources .And many researchers also proposed to represent EC points by using different projective coordinates forms instead of the usual affine form. Researchers found that using projective coordinates eliminates inversion operation by converting it to several multiplication operations. Hence, ECC can perform its. Computations with no inversion operation using projective coordinates form.[6].

2. Literature Survey

In this paper the Anoop MS proposed the Implementation of ECC using Jacobian projective coordinates has shown considerable improvement in efficiency compared to the affine coordinate implementation. This improvement in efficiency is due to the elimination of multiplicative inverse operation in point addition and doubling that would otherwise cost considerable processor cycles [5]. In this paper The T. Abdurahmonov, Eng-Thiam Yeoh, and Helmi Mohamed Hussain propose the Elliptic curve exponentiation include in coordinate systems of elliptic curve cryptography that coordinate systems will be implemented in the global smart card such as encryption and digital signature. In these coordinate systems consists of two points which is point addition and point doubling. Coordinate systems are Affine, projective, Jacobian, Jacobian-Chudnovsky and the modified Jacobian coordinates. These coordinate systems are mixed that one coordinate system has occurred what to implement prime field (Fp) over elliptic curve cryptography in global smart cards. As a result of mixed coordinate system [4]. In this paper The Muhammad Yasir Malik Proposed implementation takes only fraction of a second Along with time consumption ECC provides power consumption too. This makes it an ideal choice for portable, mobile and low power applications. It can be a very secure and useful replacement of already being used crypto systems for key exchange, key agreement and mutual authentication (like RSA, EIGamal and their variants). Its use can be further extended in smart cards and RFID applications because of less memory and low power requirements [7].

In this paper the Adnan Abdul-Aziz Gutub This study targeted speeding-up elliptic curve crypto (ECC) computations. We focused on ECC scalar multiplications adopting projective coordinates to reduce the inversion complexity effect. The study proposed remodeling Jacobian projective coordinate system tuned for parallel hardware implementation. We proposed merging ECC point adding and point doubling operations as a new modified method. The proposed hardware is similar to previous designs of four multipliers and an adder but with one more adder making it involve two addition units [3]. In this paper the Haodong Wang, Bo Sheng and Qun Li describe an ECC-based access control scheme in sensor networks. We give the protocol for the network to authorize a user to access the network and data collected by the sensors. We show our implementation of ECC on primary field on TelosB platform and compare the performance with other implementations that are ported to TelosB. Even though user access list authentication takes 10.1 sec, it is possible to further reduce the running time by using more refined and careful programming. Our experiment results demonstrate that public-key cryptography is feasible for sensor network security applications including access control. Our next step is to investigate more sophisticated access control schemes to alleviate the harm incurred by compromised sensor nodes [1].In this paper the Kristen Lauterproposed over the last five years, elliptic curve cryptography has moved from being an interesting theoretical alternative to being a cutting edge technology adopted by an increasing number of companies. There are two reasons for this new development: one is that ECC is no longer new, and has withstood a generation of attacks; second, in the growing wireless industry, its advantages over RSA have made it an attractive security alternative. Wireless devices are rapidly becoming more dependent on security features such as the ability to do secure email, secure Web browsing, and virtual private networking to corporate networks, and ECC allows more efficient implementation of all of these features [2].

3. Public Key Cryptosystem

Elliptic curve cryptography [ECC] is a public__key cryptosystem just like RSA Public-key cryptography has been used extensively in data encryption, digital signature, user authentication, etc. Public-key cryptography provides a more flexible and simple interface requiring no key redistributions, no pair wise key sharing, no complicated one-way key chain scheme. . The recent progress in 160-bit Elliptic Curve Cryptography (ECC) shows that an ECC point multiplication takes less than one second, which proves public-key cryptography is feasible. In recent years, ECC has attracted much attention as 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. [1] Public-key schemes are typically used to transport or exchange keys for symmetric-key ciphers. Since the security of a system is only as good as that of its weakest component, the work factor needed to break a symmetric key must match that needed to break the public-key system used for key exchange [9]

4. Elliptic Curve Cryptosystem

Elliptic curve cryptosystem is proposed by miller and koblitz in 1985.It is most popular public key cryptosystem till date. Elliptic curve define over finite field Prime number [Fp] where p is the prime number The mathematical operations of ECC is defined over the elliptic curve y2 = 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. [4]

The elliptic curve group operation is closed so that the addition of any two points is a point in the group. Given two points P and Q, with the coordinates (x1, y1), (x2, y2), respectively, the addition results in a point R on the curve with coordinate (x3, y3), where x3 and y3 satisfy
(x1, y1) + (x2, y2) = (x3, y3) [1]
General equation of elliptic curve is
y2 = x3 + ax + b,

Addition of two points in ECC

Such that
x3=λ^2-x1-x2,
y3=λ l(x1-x3)-y1,
Whereλ= (y2-y1)/(x1-x2) [3]

Doubling formula of two point in ECC
X3=λ^2-2x1,
y3=λ(x1-x3)-y1,
Where λ= (3$x1^2$+a)/ (2y1)

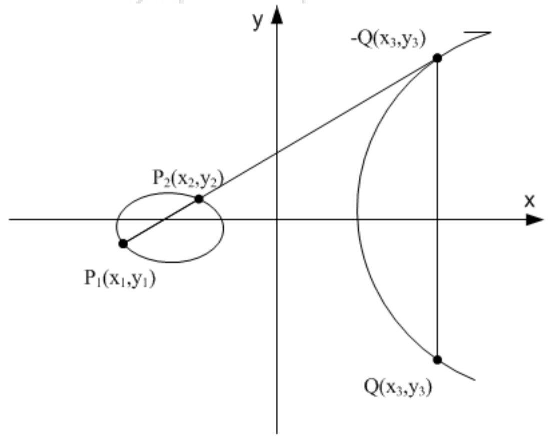

Figure 1: Point addition in E [Fp]

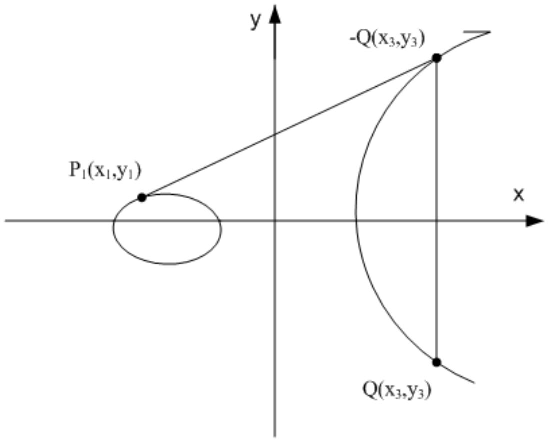

Figure 2: Point doubling in E [Fp]

5. Jacobian ECC

For Jacobian coordinates, we set $x=X/Z^2$ and $y= Y/Z^3$, giving the equation:
Ep: $y^2=x^3+a XZ^4+bZ^6$ (mod p), [3]
Let P=(X1, Y1, Z1), Q=(X2, Y2, Z2) and
P+Q=(X3, Y3, Z3) be points of E (GF (p)),

Addition formula:
$X3=-H^3-2U1H^2+r^2$
$Y3=-S1ZH^3+r(U1H^2–X3)$,
Z3=HZ1Z2
Where,
$U1=X1Z2^2$,
$U2=X2Z1^2$
$S1=Y1Z2^3$,
$S2=Y2Z1^3$
H=U2-U1,
r=S2-S1

Doubling formula:

X3=T,
$Y3=-8y1^4+M(S-T)$,
Z3=2Y1Z1
Where,
$S = 4X1y1^2$
$M=3x1^2+aZ1^2$
$T= -2S+M^2$

6. ECC Versus JECC

Projective and weighted projective (also called Jacobian) coordinates are sometimes used, especially in cases where division in the underlying field is costly. Weighted projective coordinates work with triples of coordinates (x, y, z), corresponding to the affine coordinates (x/z2, y/z3) whenever $z \neq 0$. The advantage of weighted projective coordinates is that point addition on the elliptic curve can be done in 16 field multiplications, avoiding all field divisions. Field divisions in prime fields are often reported to be roughly 80 times as costly computationally as multiplications in the field. Such a ratio would clearly indicate the use of weighted projective coordinates instead of affine coordinates [2]

The other two ECC scalar multiplication modular operations are inversion and multiplication. Inversion is known to be the complex and very expensive operation , its cost is reduced by converting the normal (x, y) affine coordinate system to projective coordinate system (X,Y,Z)[3]

Implementation of ECC using projective coordinates has shown considerable improvement in efficiency compared to the affine coordinate implementation. This improvement in efficiency is due to the elimination of multiplicative inverse operation in point addition and doubling that would otherwise cost considerable processor cycles [5]

Many researches proposed to represent EC points by using different projective coordinate's forms instead of the usual affine form. Researchers found that using projective coordinates eliminates inversion operation by converting it to several multiplication operations. Thus, ECC can perform its Computations with no inversion operation using projective coordinate's form, which contributes to enhance the Performance of ECC algorithm [6]

Projective coordinates are preferred over affine coordinates to represent points on an elliptic curve. Points can also be represented with their x-coordinate only. Point multiplication is then evaluated via Lucas chains .This avoids the evaluation of the y-coordinate, which may result in improved overall performance Yet another technique to speed up the computation is to use additional point addition and doubling that would otherwise cost considerable processor cycles [7].

Finding multiplicative inverse (Modular Inversion) operation is the most time-consuming operation in Elliptic Curve Crypto-system (ECC) operations which affects the performance of ECC .Moreover, several factors that affect the design of ECC have not been intensively investigated in the Majority of researches related to ECC, Such as system utilization, area, resources-consuming and area*time cost factors, which play significant role in designing efficient ECC for different applications [6].

7. Conclusion

In recent years, ECC has attracted much attention as the security solutions 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 Scalar multiplication method itself .The choice of the field definition impacts the performance of the underlying field arithmetic: addition, multiplication and inversion. There are two types of coordinator used , Jacobian coordinates and affine coordinator .the Jacobian coordinators are preferred over affine coordinate because the Jacobian coordinator improved the efficiency and maintain the cost hence the paper proposed how the Jacobian coordinators are better than the affine coordinator

References

[1] Haodong Wang, Bo Sheng and Qun Li," Elliptic curve cryptography-based access control in sensor networks", Int. J. Security and Networks, Vol. 1, Nos. 3/4, 2006
[2] Kristen Lauter, Microsoft Corporation "The Advantages of Elliptic Curve Cryptography for Wireless Security", IEEE Wireless Communications • February 2004
[3] Adnan Abdul-Aziz Gutub "Remodelling of Elliptic Curve Cryptography Scalar Multiplication Architecture using Parallel Jacobian Coordinate System," International Journal of Computer Science and Security (IJCSS), Volume (4): Issue (4)
[4] T. Abdurahmonov, Eng.-Thiam Yeoh, and Helmi Mohamed Hussain " A Proposed Implementation of Elliptic Curve Exponentiation over Prime Field (Fp) in the Global Smart cards," International Journal of

Information and Electronics Engineering, Vol. 3, No. 1, January 2013

[5] Anoop MS," Elliptic Curve Cryptography An Implementation Guide", Elliptic Curve Cryptography – An Implementation Tutorial

[6] Mohammad Alkhatib, AzmiJaafar, ZuriatiZukerman, Mohammad Rushden, MD. SAID "The Design of Projective Binary Edwards Elliptic Curves over GF (P) benefiting from mapping elliptic curves computation to variable degree of parallel design" ISSN: 0975-3397 Vol. 3 No. 4 Apr 2011

[7] Marc Joye, Thomson R&D France, "Fast Point Multiplication on Elliptic Curves without Precomputation" Published in J. von zur Gathen, J.L. Ima~na, and C» .K. Ko»c, Eds, Arithmetic of Finite Fields (WAIFI 2008), vol. 5130 of Lecture Notes in Computer Science, pp. 36{46, Springer, 2008.

[8] Vipul Gupta, Douglas Stebila_, Stephen Fung, Sheueling Chang Shantz, Nils Gura, Hans Eberle "Speeding up Secure Web Transactions Using Elliptic Curve Cryptography," Sun Microsystems, Inc.2600 Casey Avenue MountainView,CA94043http://research.sun.com/projects/crypto

[9] Avinash Wadhe, Rahul Suryawanshi, Nikita Mahajan "Novel Approach for Worm Detection using Modified Crc32 Algorithm" National Conference on Innovative Paradigms in Engineering & Technology (NCIPET-2012) Proceedings published by International Journal of Computer Applications® (IJCA)

[10] Prof.Avinash Wadhe, Miss Namrata A. Sable "Mobile SMS Banking Security Using Elliptic Curve Cryptosystem in Binary Field," International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 3, May-Jun 2013, pp.413-420

[11] Lekha Bhandari, Mr.Avinash Wadhe " Speeding up Video Encryption using Elliptic Curve Cryptography (ECC)" 2013 Bhandari Page 24 International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-2, Issue-3)

Author Profile

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 Digital Forensics, Network Security, Data mining and Cloud Computing .He has contributed to more than 20 research paper. He had awarded with young investigator award in international conference.

Anagha P. Zele received the BE from SGBAU Amravati University and pursuing ME (CSE) From G. H. Raisoni College of Engineering & Management, Amravati. Her Research interest include Network Security