Java Implementation And Arithmetic Performance Evaluation of Elliptic Curve Cryptography Using MATLAB

Amanpreet Kaur
M.Tech scholar
SBSSTC, Ferozepur

Vikas Goyal
Assistant Professor CSE deptt.
MIMIT, Malout

Pawan Luthra
Assistant Professor CSE deptt.
SBSSTC ,Ferozepur

Abstract

Cryptography technology exists to protect the data during transmission over any channel of communication like internet.Elliptic curve Cryptography in terms of accuracy and fast observation of results for better security solution.Elliptic Curve security aspect and to maintain the curve with positive and accurate observation is really hard to apply.ECC is public key cryptography so, it also gives introduction to projective coordinate system and shows why finite fields are introduced as comparing to RSA , DSA, AES cryptosystems. Analysis of ECC is observer over key size and encryption time available over the specific system or application, but for accurate observation we do analysis on basis of type of key or category of cryptographic primitives used to solve given mathematical problem. ECC and other public key cryptographic algorithms have basic criteria of production of keys and method of encryption and decryption in basic application as per base of basic security properties like authentication, non-repudiation, privacy, integrity.

Keywords:ECC, RSA, Cryptography, Field, Primitives.

1. Introduction

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription [5]. Elliptic curve Cryptography (ECC) in which each user and device taking part in communication uses the pair of public and private key.as we know cryptography technology refers to security of system so it deals with many properties.The process of proving one's identity is Authentication.. Public key cryptography are based on computational difficulty of various problems, numerical algorithms are used for solving these difficulties. Cryptanalysis is also a modern cryptography technology used to find some weakness and Insecurity in cryptographic scheme. CryptosystemOne or more cryptographic primitives are often used to develop a more complex algorithm called cryptographic system and cryptosystem. Cryptography is usually subdivided into two major classes: entity authentication and data origin authentication Cryptography provides mechanisms for such procedures.[1,2]

2. Elliptic curve cryptography(ECC)

Elliptic curve cryptography (ECC) was invented by Neal Koblitz and Victor miller in 1985. They can be viewed as elliptic curve analogues of older discrete logarithm(DL) cryptosystem. Mathematical basis for security of elliptic curve cryptography is computational intractability of elliptic curve discrete logarithm problem (ECDLP)[7].

Using elliptic curve cryptography instead of traditional IFP or DLP based cryptography has some relevance when using a low cost standard smart card. ECC offers smaller key size and the implementation are therefore potentially faster. Furthermore smaller keys take less storage, which is important because smart cards have limited memory to use. On other hand using ECC has some obvious drawbacks: ECDLP has not been analysed long form the security point of view and this may cause some problem in future. ECC mathematics is somewhat more advanced and it has not been studied as long as widely as traditional Arithmetic's.

2.1 Protocols of Elliptic Curve Cryptography

Design of a special purpose processor with elliptic curve digital signaturealgorithm (ECDSA) functionality design parameters were low energy consumption, small chip area, robustness against cryptographic attacks, and flexibility. The asymmetric cryptosystem allows authentication of the tag to untrusted third parties without revealing the secret key. The ECDSA functionality was implemented using a prime field GF(p) and affine coordinates, an alternative way to reduce the die size and the costs of the tag. The standard-cell based implementation of the device is fully scalable for different prime fields sizes[4,8]. This paper describes the implementations and test results of elliptic curve cryptography (ECC) and elliptic curve digital signature algorithm (ECDSA) algorithms based on Java card. A 163-bit ECC guarantees as secure as the 1024-bit Rivest-Shamir-Adleman (RSA) public key

algorithm, which has been frequently used until now.ECC is more appropriate for use on secure devices such as smart cards and wireless devices with constrained computational power consumption and memory resources.

Elliptic Curve Diffie-Hellman approach (ECDH) is an elliptic curve version of Diffie- Hellman key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel.

Elliptic Curve Authentication Encryption Scheme(ECAES) is a version of elliptic curve criteria, used for authentication as security purpose.In all the protocols that are discussed, the most consuming part of the computation are scalar multiplications. That are calculated of the form

$$Q = k * P = P + P + P + P \ldots . k\ times$$

Here P is a curve point , k is a integer in range of order of P. P is fixed point that generate a large, prime subgroup of $E(F_P)$, or P is an arbitrary point in such a subgroup. Elliptic Curves have some properties that allow optimization of scalar multiplication.

2.2Utilization of Elliptic Curve Cryptography

Solution of DLP can be computed faster than that of ECDLP. This property of elliptic curve makes it favorable for its use in cryptography. Elliptic curve cryptography has developed in which security is based on number theoretic problem solving elliptic curve. Fast execution time, smaller memory consumption and saving in band width have made ECC an attractive public key solution .One of the main ECC primitives is scalar point multiplication , which is basic building block in many security protocols.

Let E be elliptic curveand $P \in E$ be point of order n. Given a point $Q \in E$ with

$Q = m * P$for certain $m \in \{2,3, \ldots \ldots, m-2\}$.

Difference in ECDLP and DLP is that, DLP though a hard problem is known to have a sub exponential time solution of DLP can be faster than to be ECDLP. This property ofElliptic Curve makes it more useful in many applications.

3.Introduction to Elliptic Curve Arithmetic

An abelian group is a set A, together with an operation "•" that combines any two a and b to form element another element denoted $a \bullet b$[7]. The symbol "•" is a general placeholder for a concretely given operation. To qualify as an abelian group, the set and operation, $(A, \bullet)$, must satisfy five requirements known as the abelian group axioms:Closure, Associativity, Identity element, Inverse element**,** Commutative. More compactly, an abelian group is a commutative group. A group in which the group operation is not commutative is called a "non-abelian group" or "non-commutative group". A number of public key cipher are based on use of an abeliangroup[3]. For cryptography the variables and coefficients are restricted to elements in a finite field, which results in the definition abelian group. Suite of large integer arithmetic operations including addition, subtraction, shift, multiplication, divison and modular reduction.

3.1 Finite Field: Taxonomy

The elliptic curve operations are defined above are on real number. Operations over the real number are slow and inaccurate due to round-off errors. Cryptographic operations need to be fast and accurate. To make operation on elliptic curve accurate and more Efficient, the curve cryptography is defined over two finite fields: Prime field, Binary field. A finite field consists of a finite set of elements together with two binary operations called addition and multiplication, which satisfy certain arithmetic properties. Elliptic Curves Operations over Finite Fields require main operation is Point multiplication is achieved by two basic elliptic curve operationsPoint addition, Point doubling.

4. Applications of ECC

Many devices are small and have limited storage and computational power[14]. Where can we apply ECC? Smart cards, Web servers that need to handle many encryption sessions, Wireless communication devices. Any application where security is needed but lacks the power, storage and computational power that is necessary for our current cryptosystems. A frequency based differential Electromagnetic analysis which compute spectrogram for symmetric key cryptography avoids the large overheads , due to this reason it is also used in wireless embedded system.[14]

4.1 Problem with Elliptic curve cryptography

a) Security: The main issue is that the true difficulty of ECDLP is not fully understood. Recent research has shown that some elliptic curve that were believed suitable for elliptic curve cryptography are in fact not appropriate. For example: if the order of base point of curve equal to prime p then it turned out to be "anomalous" curve. Signature generation for ECDSA becomes significantly faster than RSA system.

Signature Verification using ECDSA is much slower than for RSA.[9]

b) Curve generation

it is extremely difficult to generate a suitable curve and base point in first place [6]. The main problem how to count points on curve? Incompatible system: The "odd" and "even" elliptic curve implementation are similar but sufficiently different to ensure that "odd" system will be incompatible with "even" system. Processing: Elliptic curve systems use small key size and less computing power.

5. ECC curve generation

Elliptic curve drawn using cubic equation got observed over the real is accurate in nature. There are many points generated using the basic criteria that is point addition and point doubling[11] .As a result generator point on which we can apply different operations for security purpose. To draw the Elliptic Curve we mentioned generator point details ,signature details for implementing digital signature ,curve points description.

Generator point	Signature
(48439561293906451759 05258525279791420276 2 94952604174799584408 0 717082404635286, 36134250956749795798 5 85127919587881956611 1 06672985015071877198 2 53568414405109)	3045022004a4f46164711 9ba966cc85f32deaf2ef98 6ee314e23db345effaf33d 1e22428022100bd473f8d 84ebe2f21bbde7c0e85acc eab21374aa42d0331e710 e233533c7b62d

Curve points
(2,7)+(7,2)=(3,5)
(2,7)+(2,7)=(5,2)
(2,7)+(2,-7)=(0,0)
(0,0)+(0,0)=(0,0)
(7,2)+(6,0)=(7,9)

6 Tables, Figures and Graphical Representation

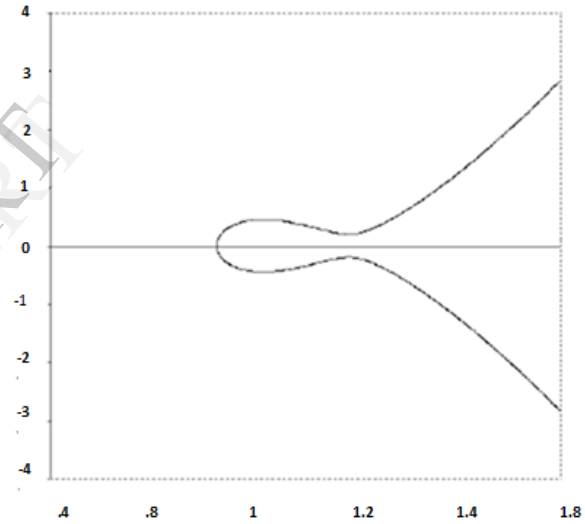
6.1 Tables

In given table, Observation of Elliptic curve cryptographic algorithm is shown. From this we get Computationally Equivalent Keys sizeratio 1:4 as compare to other public key cryptographic algorithms.

Table 1.Key size and total time readings for Elliptic curve Cryptographic algorithm

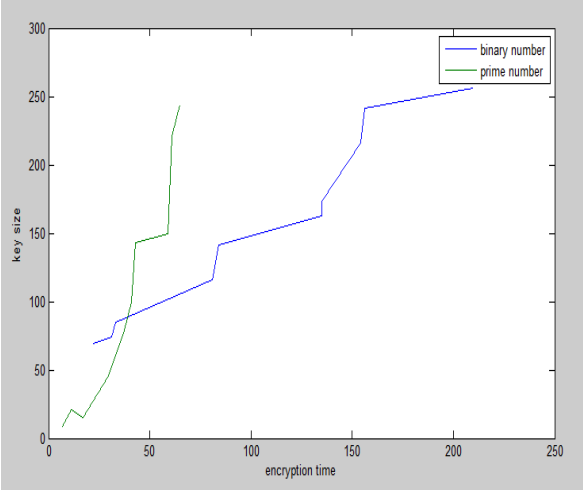
Key size	Encryption Time	Decryption Time
228 bits	50.68153	3.36551
482bits	68.21930	4.41927
620bits	72.28547	6.12233
916bits	81.96291	9.87721
1864bits	90.78851	11.1234

6.2Graphical Representation



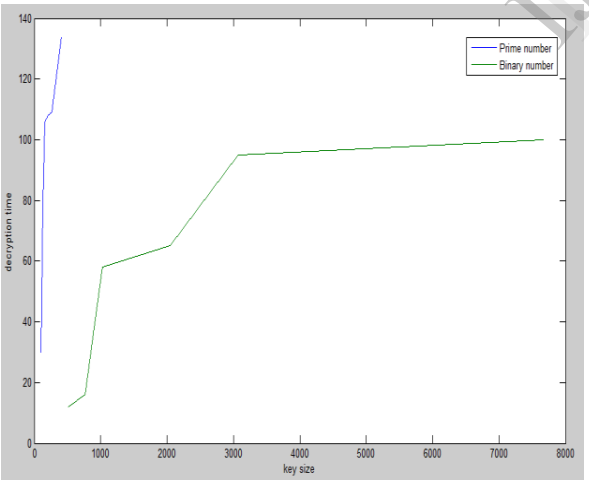
Graph 1: Graphical Representation of Elliptic Curve

Graph 1 Describes the Graphical Representation of Elliptic Curve of the form $y^2 = x^3 + ax + b$. Where the value of a and b are positive in nature.



Graph 2:key size and encryption time of Elliptic Curvecryptographic algorithm over field

Graph 2 describes the observation of Elliptic curve over fieldshows nature of ECC as binary and prime field. For the comparison prime observation factor as time, key size taken under same condition but for accurate observation finite field elements changes accordingly to base ECC algorithm.



Graph 3:key size and decryption time of Elliptic Curve cryptographic algorithm over field

Graph 3 describes the key size and decryption time of ECC, when implemented in java using MATLAB. Both graph shows that nature of prime number is better option than binary number taken under observation.

7. Previous work

For efficient implementation of ECC, it is important for multiplication algorithm and underlying field arithmetic to be efficient. There are different methods for efficient implementation point multiplication and field arithmetic suited for different hardware configuration[1]. ECC is a very encouraging and new field to work in order to find a more cost efficient method to perform encryption for portable devices and to secure image transmission over internet. These comparisons illustrate the appeal of elliptic curve cryptography especially for applications that have high security. The market for Personal Digital Assistants (PDA) is growing sharply and PDAs are becoming increasingly attractive for commercial transactions. On requirement for further growing of E-commerce with mobile devices is the provision of security[12].

8. Conclusions

Elliptic curve drawn using equation$y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$ together with a point at infinity denoted o,gives the satisfactory results in prime field and binary field, more over better in prime field compared to binary or other than that natural number using a single algorithm as base .We concluded that graph of prime is less complex comparing to binary data, in terms where time and memory is taken as primary observation for better implementation and security solution.

References

[1] Elliptic curve cryptography an implementation guide by Anoop MS anoopms@tataelxsi.co.in.

[2] CSE 450/598 Design and analysis of algorithm Project ID:P113 Elliptic Curve Cryptography by Vikram V Kumar, SatishDoraiswamy, Zabeer Jainullabudeen.

[3] Elliptic curve cryptography, datacom white papers2000.

[4] Standards for efficient cryptography " by Certicom Research September 20,2000.

[5] Applications of elliptic curves in public key cryptography" by AndrejDujella 2002.

[6] Method for breaking RSA Security by Vibhor Malhotra, Dr.K.CJoshi,,september2012,

www.ijarcsse.com.

[7] Implementation of Elliptic curve digital Signature Algorithm by Aqeel Khalique, Kuldeep Singh, SandeepSood (IIT ROORKEE) vol.2 May 2010.

[8] Suzanne Craig LiljanaBabinkostova, Elliptic Pairs of Primes in Cryptography and Their Effects on RSA Security,November,2011.

[9] The Elliptic Curve Digital Signature Algorithm by Don Johnson and Alfred Menezes, Scott Vanstone, Certicom Research Canada, University of Walterloo.

[10] Book: Cryptography and Network Security Principles and Practice, 5th Edition by William Stallings.

[11] www.cryptographyworld.com/des.html.

[12] Stallings, W. "The Advanced Encryption Standard."Cryptologia".

[13] Wiener, M. "Cryptanalysis of Short RSA Secret Exponents. "IEEE Transactions on Information Theory, vol. IT-36, 1990.

[14] EM Analysis of Rijndael and ECC on a Wireless Java-based PDA,2005,CH Gebotys, S Ho, CC Tiu