July 2014

A COMPARATIVE ANALYSIS OF ECDSA V/S RSA ALGORITHM

AMANPREET KAUR

CSE deptt., BSSTC, Ferozepur-INDIA, preeti.kaur806@gmail.com

VIKAS GOYAL

CSE deptt., BSSTC, Ferozepur-INDIA, vikas_735@yahoo.com

Follow this and additional works at: <https://www.interscience.in/ijcsi>

Part of the [Computer Engineering Commons](#), [Information Security Commons](#), and the [Systems and Communications Commons](#)

Recommended Citation

KAUR, AMANPREET and GOYAL, VIKAS (2014) "A COMPARATIVE ANALYSIS OF ECDSA V/S RSA ALGORITHM," *International Journal of Computer Science and Informatics*: Vol. 4 : Iss. 1 , Article 2.

DOI: 10.47893/IJCSI.2014.1165

Available at: <https://www.interscience.in/ijcsi/vol4/iss1/2>

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Computer Science and Informatics by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

A COMPARATIVE ANALYSIS OF ECDSA V/S RSA ALGORITHM

AMANPREET KAUR¹, VIKAS GOYAL²

¹M.Tech Research Scholar, ²Assistant Prof. CSE deptt., BSSTC, Ferozepur-INDIA
E-mail: preeti.kaur806@gmail.com, vikas_735@yahoo.com

Abstract- Elliptic curve Cryptography with its various protocols implemented in terms of accuracy and fast observation of results for better security solution. ECC applied on two finite fields: prime field and binary field. Because it is public key cryptography so, it also focus on generation of elliptic curve and shows why finite fields are introduced. But for accurate observation we do analysis on category of cryptographic primitives used to solve given security problem. RSA & ECDSA both have basic criteria of production of keys and method of encryption and decryption in basic application as per security and other properties which are authentication, non-repudiation, privacy, integrity.

Keywords- ECC, RSA, Cryptography, Prime Field, Binary field, ECDSA, 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 [2]. 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. Public key cryptography are based on computational difficulty of various problems, numerical algorithms are used for solving these difficulties. Mathematical basis for security of elliptic curve cryptography is computational intractability of elliptic curve discrete logarithm problem (ECDLP)[7].

Cryptanalysis is also a modern cryptography technology used to find some weakness and Insecurity in cryptographic scheme.[2] Cryptosystem One or more cryptographic primitives are often used to develop a more complex algorithm called cryptographic system and cryptosystem.

- What is cryptographic primitives? Algorithm with basic cryptographic Properties and relationship to other cryptographic problem. [1].
 - a) Type of operation used for transforming data: Mainly two basic principal used are: Substitution and transposition.
 - b) Number of keys used: system referred to Symmetric, single, secret and conventional keys or we can say public and private keys.The transformation of data into a form that is as close to impossible as possible to read without the appropriate knowledge (a key) is encryption. Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data.[4] Elliptic curve are not ellipse, these are cubic curves .Properties of ECC made it stronger against various attacks in wireless sensor networks and many other

wireless suitable environments. Paper shows the equivalent of key sizes of RSA and ECC.

2. INTRODUCTION TO ELLIPTICAL CURVE ARITHMETIC

An Abelian group is a set A , together with an operation " $\bullet$ " that combines any two a and b to form element another element denoted $a \bullet b$. The symbol " $\bullet$ " 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:[8] Closure For all a, b in A , the result of the operation $a \bullet b$ is also in A .

Associativity For all a, b and c in A , the equation $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ holds.

Identity element There exists an element e in A , such that for all elements a in A , the equation $e \bullet a = a \bullet e = a$ holds.

Inverse element For each a in A , there exists an element b in A such that $a \bullet b = b \bullet a = e$, where e is the identity element.

Commutative For all a, b in A , $a \bullet b = b \bullet a$.

2.1 Elliptic Curve Over Prime Field

Let p be a prime number. The finite field F_p called a prime field, is comprised of the set of integers $\{0, 1, 2, \dots, p-1\}$ with the following arithmetic operations:

Addition: If $a, b \in F_p$ then $a+b=r$, where r is the remainder when $a + b$ is divided by p and $0 \leq r \leq p-1$ known as addition modulo p .

Multiplication: If $a, b \in F_p$ then $a \cdot b=s$, where s is the remainder when $a \cdot b$ is divided by p and $0 \leq s \leq p-1$ known as multiplication modulo p .

Thus, the ECC offered remarkable advantages over other cryptographic system.

- It provides greater security for a greater key size.
- It provides effective, compact implementations for cryptographic operations requiring smaller chips.

- Due to smaller chips less heat generation and less power consumption.
- It has easier hardware implementations.

3. RSA ALGORITHM

Ron Rivest, Adi Shamir, Len Adleman first published this algorithm in 1978. This is most widely accepted and implemented general purpose approach to public key encryption. In RSA Scheme is block cipher in which plain text and cipher text are Integer between 0 and $n-1$ for some n , typical size for n is 1024 bits[6]. In RSA algorithm plain text is encrypted in blocks with each block having binary value less than some number n .

Hardness of RSA is related to integer factorization problem. Given a number that is product of two large prime numbers, factorize the number to find the primes.

3.1 RSA key generation

Given the “public exponent” e , generate two prime number p and q , such that $(p-1)$ and e have no common divisor greater than 1 and $(q-1)$ and e have no prime divisor greater than 1.

Let $n = p \cdot q$, product of p and q solve $e \cdot d = 1 \pmod{(p-1)(q-1)}$

public key is pair of (n, e) private key is pair of (n, d)

3.2 RSA Encryption and decryption

Encryption uses the public key, so the cipher text corresponding to plain text m is $c = m^e \pmod{n}$

Decryption uses the corresponding private key, so $m = c^d \pmod{n}$ In simple terms signature generation is equivalent to decryption and signature verification is same as encryption.

4. 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. Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the schemes, which is beneficial to systems where real time performance is a critical factor.

5. IMPLEMENTATION AND GRAPHICAL REPRESENTATION

For efficient implementation of ECC, 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. Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the schemes, which is beneficial to systems where real time performance is a critical factor. We have estimates of parameter sizes providing equivalent levels of security for RSA and ECC systems[9]. We implemented the ECDSA algorithm of key generation, message signing and signature verification.

A. Tables

Given table shows the equivalent key size of both the algorithms that is 25 bits, comparison of key size of Elliptic curve cryptography (ECC) and RSA algorithm is represented:

Table1.key sizes of ECC & RSA

ECC(in bits)	RSA(in bits)
106	512
112	768
132	1024
160	2048
210	3072
283	7680
409	15360
571	21000

Above table describes key size of RSA algorithm and Elliptic Curve Cryptography (in bits) which described one of protocol as ECDSA. In most cryptosystem, the messages are mapped into numerical value upon which we perform mathematical operation. In ECC we need a method for mapping a message onto an elliptic curve. The problem of encoding plaintext message as points on an elliptic curve is not as simple. In particular, there are probabilistic methods for finding points that can be used for encoding message [7].

Table2: Comparison of RSA and ECDSA

Algorithm	Encryption Time	Key Strength
RSA	4ms	Less than 2ms
ECDSA	71ms	33ms

RSA	3ms	5ms
ECDSA	63ms	70ms
RSA	7ms	4ms
ECDSA	41ms	92ms

Graph 3: Decryption time v/s key size

6. CONCLUSIONS

Elliptic curve drawn using cubic equation gives the satisfactory results in prime field and binary field. By using Finite field in one of protocol of ECC that is ECDSA, when compared to Big integer Prime numbers using single algorithm as base i.e RSA (Ron Rivest, Adi Shamir, Len Adleman) algorithm using GMP library concluded that graphs gives the complexity of both the algorithms and as a result system, implemented in java, has been proven more accurate and stronger as compared to RSA in terms of other important factor shorter key size and bigger key strength.

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, Satish Doraiswamy, 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 Andrej Dujella 2002.
- [6] Method for breaking RSA Security by Vibhor Malhotra, Dr. K. C Joshi, September2012, www.ijarcsse.com.
- [7] Implementation of Elliptic curve digital Signature Algorithm by Aqeel Khalique, Kuldeep Singh, Sandeep Sood (IIT ROORKEE) vol.2 May 2010.
- [8] Suzanne Craig Liljana Babinkostova, 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 Waterloo.
- [10] www.cryptographyworld.com/des.html.

Graph 1: Elliptic curve points along x and y axis

Elliptic curve cryptography as shown in the figure depends on type of curve using to implement it. Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the schemes, which is beneficial to systems where real time performance is a critical factor.[10]

Graph 2: Encryption time v/s key size