An Implementation Of Elliptic Curve Cryptography

[1] P. K. Sahoo
[1]*Professor, Department of Computer Science Engineering, St. Martins Engineering College, Hyderabad-500014, (AP), India.,*

[2] Dr. R. K. Chhotray
[2] *Professor, Department of Computer Science Engineering, NIT Rourkela, Odisha-769008, India*

[3] Dr. Gunamani Jena
[3] *Professor, Department of Computer Science Engineering, BVCEC (JNTUK) AP-533210, India*

[4] Dr. S. Pattnaik.
[4] *Professor, P.G.Department of Information & Communication Technology, F.M. University, Vyasa Vihar, Balasore, Odisha-756019, India,*

Abstract

The internet is slowly becoming an increasingly dangerous mode of communication for all forms of highly sensitive data. The increased dependency by individuals, institutions and corporations over the Internet to carry out critical business processes have provided a playing field for the intruders to carry out different attacks on the system and on the network. The security to critically confidential information such as personal identity information, credit card details, online transactions and e-commerce is the need of the hour which depends on top of cryptography. It is thought that RSA is a very secure cryptography algorithm and almost all software products provide advanced data encryption are designed over it. The bit length for RSA has increased over the years to make the encryption very tough, which increases the processing time and storage requirement is the real concern for today. The objective of this paper is to propose an alternative algorithm for cryptography based on mathematical objects known as elliptic curves. The proposed algorithms provide a better security with shorter bit length than RSA. Hence elliptic curve cryptography is the only solution today where better security can be achieved with a smaller key size thereby reducing the processing overhead.

1. INTRODUCTION

1.1 Introduction to cryptography

The term cryptography is derived from the Greek word Kryptos. Kryptos is used to describe anything that is hidden, veiled, secret or mysterious. Cryptography is the art and science of hiding information in a systematic order such that only the authorized parties have access to the correct information. Cryptography is the study of mathematical techniques for the secure transmission of a private message over an insecure channel. Cryptography is defined as the study of secret writing that concerns the ways, in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers and other methods, so that only certain people can see the real message. Cryptography is used to encrypt data residing on storage devices or traveling through communication channels in order to ensure that any illegal attempt to access the data is not successful. Cryptography also

used to secure the process of authentication of different parties, who are trying to use any function on the system.

1.2 The social aspects of cryptography

In an age of explosive worldwide growth of electronic data storage and communications, many vital national interests require the effective protection of critical information. The Internet has now become the main mode of data communication and critical infrastructure for firms to carry out critical business processes. Although Internet offers several potential benefits, including improved efficiency, productivity and convenience with reduced costs, it exposes firms to new level of risks such as security breaches. The risk is more pronounced for private companies, where loss of important data could mean a tremendous advantage for the competitor. Even among the companies, the threat to pharmaceutical companies is far more serious where intellectual properties of drugs are always prone to theft. "Everyone is vulnerable. However, if I have to rank in terms of merit, the IT/BPO sector has the highest standards of security because of the pressure of foreign countries, followed by banks and then telecom," says Kamlesh Bajaj, CEO, Data Security Council of India and former head of Cert-in [1]. In 2010, as tensions rose between the West and Iran over the Iran's nuclear plants, an internet worm called Stuxnet, was discovered at Iran's nuclear enrichment centre at Natanz. The worm was attacking the computers that controlled the centre, by taking over the control of the centrifuges at the plant. It was partially successful. The worm then escaped the nuclear plant and spread over the internet, infecting computers worldwide. India was the third-most affected country, with 8.31 per cent computers affected, following Iran (58.85 per cent) and Indonesia (18.22 per cent). According to the security firm Sophos around 453491 email passwords were posted online by hacker group D33DS Company. In the biggest-ever series of cyber attacks uncovered, hackers are found to have broken into networks of the Indian government, the united nations and the U.S defense companies. Seventy-two organizations, including major US defense groups, have been victims of the cyber attack that began in 2006, making it one of the largest concerted hacking attempts in the history. The long list of victims in the five year cyber attack campaign include the government of US, India, Taiwan, South Korea, Vietnam and Canada; the Association of Southeast Asian Nations (ASEAN); the international Olympic committee (IOC), the world Anti-Doping Agency, Us energy Department labs as well as agencies and companies in Denmark, Germany, Indonesia and Singapore. The hackers also broke into the computer system of UN secretariat in Geneva in 2008, accessing the secret data for nearly two years [2]. In today's era of the ubiquitous computing, the Internet has become the main mode of data communication. Most of the devices used in wireless mobile environments, that from wireless networks, ad-hoc networks and wireless sensor networks etc. have low computational power and memory. In such a Pervasive Computing environment, providing security to data becomes a complex task [3]. There are constant occurrences of Internet security problems due to rapid development [4]. The table 1 given below shows the various security attacks from 2004 to 2010.

Table 1 shows the details of the various attacks from 2004 to 2010.

Security Incidents	2004	2005	2006	2007	2008	2009	2010
Phishing	3	101	339	392	604	374	508
Network Scanning /Probing	11	40	177	223	265	303	477
Virus/Malicious Code	5	95	19	358	408	596	1817
Spam	--	--	--	--	305	285	981
Malware Propagation	--	--	--	--	835	6548	6344
Others	4	18	17	264	148	160	188
Total	23	254	552	1237	2565	8266	10315

1.3 Types of cryptography

In private key cryptography both the sender and the receiver share the same key, that must be kept private. In order to communicate with each other, the key must be passed between them; the process is known as key distribution. The concept of public-key cryptography evolved from an attempt to attack two of the most difficult problems associated with the conventional encryption. The first problem is that of key distribution and the second problem is that of digital signatures. The public-key cryptography is asymmetric involving the use of two separate keys, in contrast to symmetric conventional encryption, which uses only one key. The public key system eliminates the key distribution process that hampers all private key systems since there is no need to communicate

secret keys among communicating parties. A public key cryptosystem is an asymmetric cryptosystem where each party has two sets of keys; the key is constructed of a public key and a private key. The public key, known to all, can be used to encrypt messages where as the other is kept secret and only known to the owner, the private key. Only a person that has the corresponding private key can decrypt the message. In a public-key cryptographic scheme, a key pair is selected so that the problem of deriving the private key from the corresponding public key is equivalent to solving a computational problem that is believed to be intractable. Number-theoretic problems whose intractability forms the basis for the security of commonly used public-key schemes are:

1. The integer factorization problem, whose hardness is essential for the security of RSA public-key encryption.
2. The discrete logarithm problem, whose hardness is essential for the security of the ElGamal public-key encryption and signature schemes and their variants such as the Digital Signature Algorithm (DSA).
3. The elliptic curve discrete logarithm problem, whose hardness is essential for the security of all elliptic curve cryptographic schemes.

1.4 Key length and encryption strength

Breaking an encryption algorithm is basically finding the key to access the encrypted data in plain text. For symmetric algorithms, breaking the algorithm means trying to determine the key used to encrypt the text. For public key cryptography breaking the algorithm means accessing the secret information that shared between the two recipients. The key strength of an algorithm is determined by finding the fastest method to break the algorithm and comparing it to a brute force attack. Encryption strength is often described in terms of size or length of the keys used to perform the encryption, longer keys generally provides stronger encryption. As an example the 128-bit RC4 encryption is $3*10^{26}$ times stronger than 40-bit RC4 encryption. An encryption key is considered full strength if the best known attack to break the key is no faster than a brute force attempt to test every key possibility. As it is relatively trivial to break an RSA key, an RSA public-key encryption cipher must have a very long key, at least 1024 bits, to be considered cryptographically strong.

2.1 RSA algorithm and cryptography

In 1977 Shamir, Rivest and Adelman proposed the first public-key cryptosystem called RSA as a principal object for public-key cryptography. RSA is known as the best algorithm for digital signatures and public-key cryptography. The RSA cryptosystem is an official standard worldwide. The International Organization for Standardization (ISO) 9796 standard lists RSA as a compatible algorithm as ITU-T X.509 security standard. The RSA is the official standard of Society for Worldwide Interlake Financial Telecommunications (SWIFT). X9.44 draft standard for the US banking standard and French Financial Industry's ETEBAC 5 Standard also accepted RSA cryptography. The RSA cryptography algorithm also built into current operating systems such as Microsoft, Apple, Sun and Novell.

2.2 Comparison between RSA and ECC

The best known algorithm for digital signatures and public-key cryptography is RSA (Rivest, Shamir & Adleman). Even though RSA is highly secure and widely used, there are many problems in its implementation. The security of RSA is thought to be equivalent to the problem of factorizing the modulus n and the size of an RSA key usually is a function of the number of bits in the modulus. The brute-force attack over RSA can be easily overcome by increasing the key size but decryption time increases 8-fold as key size double. The threat to larger key sizes is twofold: the continuing increase in computing power and the continuing refinement of factoring problem [5]. Because RSA is based on modular arithmetic with very long operands, the performance of RSA is quite slow on limited environments with low memory and processor power. Also, because there has been some progress on the factorization problem, the key sizes that are considered to be secure today are relatively long. Commonly used key size for RSA is 1024-bits. The entire processing time increases significantly as key size increase. Compared to RSA, the prevalent public-key scheme of the Internet today, Elliptic Curve Cryptography (ECC) offers smaller key sizes, faster computation as well as memory, energy and bandwidth [6]. The elliptic curve cryptography appears to offer equal security level for a far smaller key size, thereby reducing processing overhead. It is generally accepted that a 160-bit elliptic curve key provides the same level of security as a 1024-bit RSA key. The key advantages that can be gained from smaller key sizes include speed and efficient use of power, bandwidth and storage [7]. The celebrated RSA cryptosystem is the most largely deployed

cryptosystem but things are becoming to change. More and more applications propose to use the elliptic curve digital signature algorithm (ECDSA) to sign digital documents or messages [8]. In February 2005, the National Security Agency in the United States released a document known as Suite B, to recommend the use of Elliptic Curve cryptography as the basis for all cryptographic algorithms. It indicates that the current RSA cryptography is becoming more susceptible to attacks and hence is slowly becoming outdated. Many national and international organizations have acknowledged the use of elliptic curve as an official standard for cryptography. The International Organization for Standardization (ISO) has issued ISO 15946 (Information technology, Security techniques, Cryptographic techniques based on elliptic curves) Part 1 (General) , Part2 (Digital Signatures) ; Part 3 (Key Establishment) , ISO 14888 (Information technology, Security techniques, Digital Signatures with appendix) Part 3 (Discrete logarithm based techniques) [9-12]. The American National Standard Institute (ANSI) also standardized the use of elliptic curves such as X9.62 (Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signatures Algorithm (ECDSA) and X9.63 (Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptical Curve Cryptography) [13]. The Institute of Electrical and Electronics Engineers (IEEE) has also issued P1363 (Standard Specifications for Public Key Cryptography) and P1363a amendment of P1363 as the standard for the use of elliptic curves [14]. The development of elliptic curve cryptography is the greatest and perhaps the only true revolution in the entire history of cryptography. To quote, Lang "it is possible to write endlessly on Elliptic Curves (This is not a threat)" [15].

3.1 Introduction to Elliptic Curve Cryptography

Even though elliptic curves cryptography (ECC) has been studied for more than a hundred years, their practical aspect in public key cryptography was independently invented by Koblitz and Miller in 1984 [16,17]. Since then elliptic curve cryptography (ECC) has drawn more attention of different research communities. Because of the hardness of the elliptic curve discrete logarithm problem over that of other public key cryptographic algorithms, such as RSA and ElGamal Elliptic Curve Cryptosystems (ECCs) have been recently attracting increased attention [18]. Originally pursued mainly for aesthetic reasons, elliptic curves have recently become a tool in several important applied areas, including coding theory, pseudorandom bit generation; digital certificates in web server authentication and number theory algorithms. The elliptic curve cryptography appears to offer equal security level for a far smaller key size, thereby reducing processing overhead. It is generally accepted that a 160-bit elliptic curve key provides the same level of security as a 1024-bit RSA key.

Table 2: Shows parameter key-sizes for comparable strength of ECC and RSA

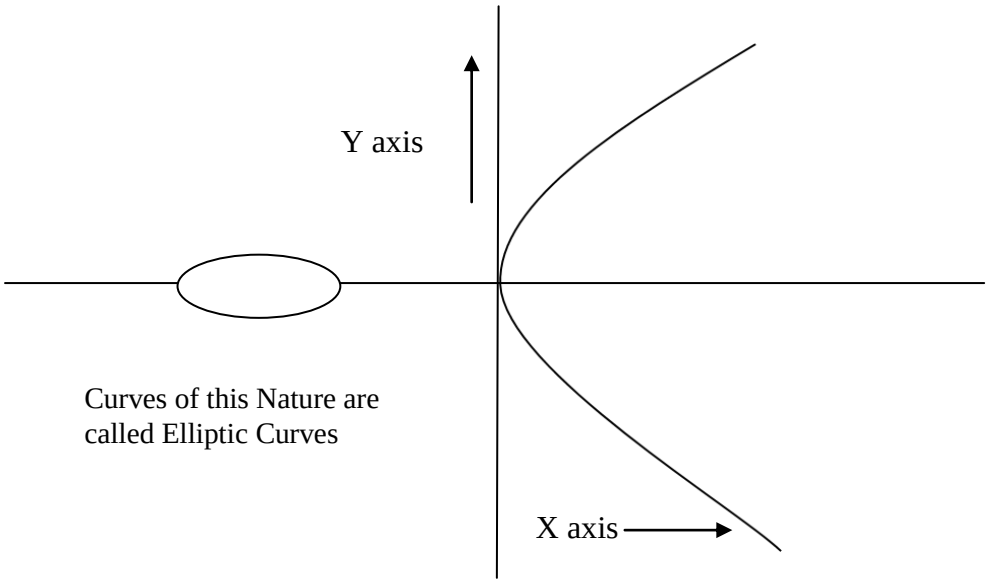
Elliptic Curve Cryptography Key-Size	RSA Key-Size	Key-Size Ratio
106 bits	512 bits	1:4
132 bits	768 bits	1:5
160 bits	1024 bits	1:6
224 bits	2048 bits	1:9
256 bits	3072 bits	1:12
384 bits	7680 bits	1:20

The table 2 shown above is the comparison between the Elliptic Curve Cryptography and RSA in terms of key size for the same security level.

Elliptic curve cryptography (ECC) is a public key cryptography system superior to the well known RSA cryptography: for the same key size, it gives a higher security level than RSA [19].

3.2 Mathematical Backgrounds of ECC

Elliptic curves are not ellipses. The name is given as elliptic curves because these are described by cubic equations, similar to those used for calculating the circumference of an ellipse. The cubic equations for elliptic curves are of the form $y^2 + axy + by = x^3 + cx^2 + dx + e$, where a, b, c, d and e are real numbers that satisfy some simple conditions.



Elliptic curve cryptographic algorithms are implemented using point operations on the Elliptic curve: Addition, doubling a point and scalar multiplication. The basic mathematics required to understand elliptic curves cryptography is discussed below.

3.3 MODULAR ARITHMETIC

Given any positive integer n and any nonnegative integer a, if we divide a by n, we get an integer quotient q and an integer remainder r that follows the below relation

$A=qn + r \quad 0 \leq r < n; \quad q=[a / n]$ and $r= a \bmod n$. Two integers a and b are said to be congruent modulo n, if $(a \bmod n) = (b \bmod n)$. This is written as $a \equiv b \pmod n$. Modular arithmetic fixes an integer $n > 1$ called the modulus. The fundamental operation in the context of modular arithmetic is the reduction modulo n.

3.4 GROUPS

Let G be a non-empty set and * be a binary operation on G. A group G sometimes denoted by $< G, * >$ is a set of elements with a binary operation denoted by *, that associates to each ordered pair (a, b) of elements in G an element (a * b) in G, such that the following axioms are hold:

(1) Associative: a* (b*c) = (a*b)*c for all a, b, c in G.
(2) Identity element: there is an element e in G such that a*e=e*a=a for all a in G.
(3) Inverse element: for every a in G, there is an element a' in G such that a*a'=a'*a=e.
(4) Closure: if a and b belongs to G, then a*b also belongs to G.

A group G is said to be commutative or abelian if ab=ba for all a, b in G.

3.4.1 CYCLIC GROUPS

A group G is said to be cyclic if there exists an element g in G such that every element a of G is an integral power of g, that is a is of the form g^n for some integer n. Then the element g is called a generator of the group. For any element a in G, we define the integral power of a as: $a^0 =e$, $a^1=a$, $a^2 =a*a$, $a^3 =a*a*a$. A cyclic group G generated by g is represented by $< g >$.

3.5 FINITE FIELDS

A field F, sometimes denoted by {F, +, *}, is a set of elements with two binary operations, called addition and multiplication, such that for all a, b, c in F the followings are hold

1. $+: F \times F \rightarrow F$ and $*: F \times F \rightarrow F$.
2. (F, +) is an abelian group.
3. (a + b) * c = a * c + b * c.
4. (F,\ {0}, *) is an abelian group.

A finite field is a field with finitely many elements. It is denoted by GF(p) or Fp. It is a fundamental theorem of the theory of finite fields, that a finite field of $p = q^m$ elements exists if and only if p is a

prime power that is q is prime and m is an integer with $m \geq 1$.

Then Fp = {0, 1, 2,……, p-1) denote the set of integers modulo p, where p is a prime number. Then (Fp, +), where the operation + is defined to be addition of integers modulo p, is a finite additive group of order p with (additive) identity element 0. In addition to this, for a given prime power p there exist essentially only one finite field Fp. In Cryptography applications, two classes of fields are commonly used. They are as follows:

- Prime fields: GF(p) or Fp, where p is prime.
- Binary fields GF(2^m), where m is large.

In elliptic curve cryptography, we are concerned with a restricted form of elliptic curve that is defined over a finite field.

3.6 ELLIPTIC CURVES OVER FINITE FIELD (Fp)

Let E be an elliptical curve over Fp. From the point of view of cryptography we are interested in elliptic curve group mod p, where p is a prime number. Then E may be described as $4a^3 + 27b^2 \pmod p \neq 0$, where a and b are two positive integers less than the prime number p. Then E_p (a, b) denotes the elliptic group mod p, whose elements (x, y) are pairs of positive integers less then p satisfying $y^2 \equiv x^3 + ax + b \pmod p$ together with the point at infinity O. As an example, if E is an elliptic curve over F7 describing by the equation $y^2=x^3+2x+4$, then the points on E are E(F7)={∞, (0,2), (0,5), (1,0), (2,3), (2,4), (3,3), (3,4), (6,1), (6,6)}. Now there is a well-known method for adding two elliptic curve points (x1, y1) and (x2, y2) to produce a third point on the elliptic curve.

3.7 Security Level Test by Certicom Pvt. Ltd

Much like the RSA challenge, the Certicom Elliptic Curve Cryptography (ECC) challenge offers prize money for finding various key sizes of the ECDLP. The current record was set in November 2002 where a 109-bit encryption key was broken with 10,000 computers running 24 hours a day for 549 days. The Certicom ECC challenge website reports that breaking a 163-bit key, which is the standard applied to most commercial ECC applications that Certicom uses, would be a hundred million times harder than breaking the 109-bit key. It is worthy to note that a 160-bit ECC key has about the same level of security as a 1024-bit RSA key. The comparison in key lengths of RSA, DSA and ECC are shown in the graph (Fig 2) below. In RSA a public key is constructed by multiplication of two very large primes. To completely break RSA one needs to find the prime factors. Clearly, ECC keys take much more effort to break compared to RSA and DSA keys. Due to this, many people believe that ECDLP is intrinsically harder than the other two problems. The most important difference between ECC and other conventional cryptosystems is that for a well-chosen curve, the best method currently known for solving the ECDLP is fully exponential, while sub-exponential algorithms exist for conventional cryptosystems.

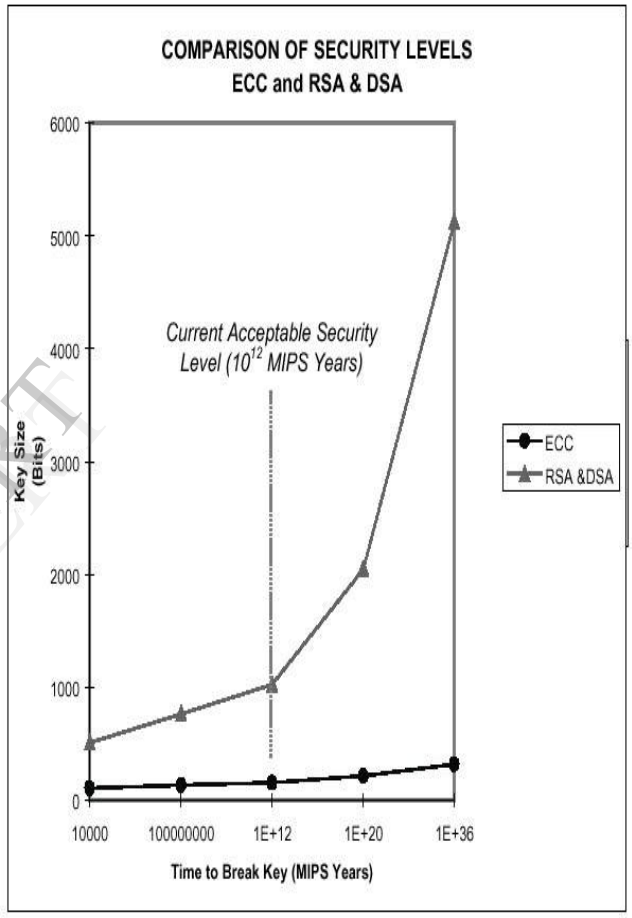


Figure 2: shows comparative study of ECC and RSA/DSA

As shown in the above figure 2 clearly proved that the algorithm based on Elliptic Curve Cryptography takes much more time to break as compared to algorithm based on RSA and DSA for the same key-size. The security of Elliptic Curve Cryptography depends on how much difficult it is to determine k given the value of kP and P. Hence Elliptic Curve Cryptography is fully exponential.

4. ELLIPTIC CURVE CRYPTOGRAPHY

4.1 ELLIPTIC CURVE KEY GENERATION

Let E be an elliptic curve over finite field Fp. Let P be a point on E (Fp) and suppose that P has prime order n. Then the cyclic subgroup of E (Fp) generated by P is <P>= {∞, P, 2P, 3P…….(n-1)P}. The prime p, the equation of the elliptic curve E, and the point P and its order n are the public domain parameters. A private key is an integer d that is selected uniformly at random from the range [1, n-1], and the corresponding public key is Q=d*P.

Algorithm 1 Elliptic curve key pair generation

Input:	Elliptic curve domain parameters (p, E, P, n).
Output:	Public key Q and private key d.
1.	Select d € R [1, n-1].
2.	Compute Q= d*P.
3.	Return (Q, d).

4.2 ELLIPTIC CURVE ENCRYPTION/DECRYPTION

The first task is to encode the plain text message m to be sent as an x-y point P_m. It is the point P_m that will be encrypted as a cipher text and subsequently decrypted. To encrypt and send a message P_m to B, A chooses a random positive integer k and produces the cipher text C_m = {kP, P_m + k Q}, where Q is B's public key. The sender transmits the points C1= kP, and C2= P_m + k Q to the recipient. To decrypt the cipher text, B multiplies the first point in the pair by B's secret key and subtract the result from the second point as P_m + k Q -d (kP) = P_m + k (dP) - d (kP)= P_m.

Algorithm 2 Elliptic curve encryption

Input:	Elliptic curve domain parameters (p, E, P, n), public key Q, Plain text m.
Output:	Cipher text C_m.
1.	Represent the plain text m as a point P_m in E (Fp).
2.	Select k € R [1, n-1].
3.	Compute C1= K*p
4.	Compute C2= P_m + k*Q.
5.	Return (C1, C2).

Algorithm 2 Elliptic curve decryption

Input:	curve domain parameters (p, E, P, n), private key d, Cipher text C_m.
Output:	Plain text m.
1.	Compute P_m = C2-dC1.
2.	Return (P_m).

5. CONCLUSION

The potential hackers are using Internet as a platform to perform various attacks over the network, the system and the society as a whole. There are continuous report of tempering of individuals confidential information and organizations vital data. Security- related threats are becoming disrupting and more damaging day by day and becoming the headlines for news papers and magazines. Hence providing strong security to critically sensitive data is the need of the hour. The most popular RSA algorithm is slowly becoming outdated because of its processing overhead and time complexity. Hence the only solution in public key cryptosystem is Elliptic curve cryptography, where a higher degree of security can be achieved with a smaller key size with a much less processing overhead. This paper demonstrates implementing Elliptic curve cryptography over finite fields for providing better security to critical data with less processing overhead.

6. REFERENCES

[1]. Akshat Kaushal, "Contagion: India's vulnerability to cyber attacks, A much-delayed cyber security policy is only making things worse", Business-standard, New Delhi, June 13, 2012.

[2]. **"**India faced 5-year cyber attacks the", Deccan chronicle Hyderabad edition, 4th august 2011. www.deccanchronicle.com

[3]. Vivek Katiyar, Kamlesh dutta, Syona Gupta, "A survey on Elliptic Curve Cryptography for Pervasive Computing Environment" International Journal of Computer Applications (IJCA), Article 8, November 2010.

[4]. I-Long Lin Hong-Cheng Yang Guo-Long Gu Lin, Proceedings of 37th IEEE International Carnahan Conference on Security Technology, pages 14-16, October 2003.

[5]. William Stallings, "The Security of RSA", Cryptography and Network Security Principles and Practices, 2nd edition 2005.

[6]. Nils Gura et al., Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPUs, CHES 2004, LNCS 3156, pp. 119–132, Springer Verlag, 2004.

[7]. Darrel Hankerson, Alfred J Menezes, Scott Vanstone, "Guide to elliptic curve cryptography", ISBN 0-387-95273-X.
[8]. S Qing, D Gollmann and J Zhou, ICICS, pages 348-359, 2003.
[9]. ISO/ IEC 15946-1-2008, (Information Technology, Security techniques, Cryptographic techniques based on elliptic curves) Part 1: General, 2008.
[10]. ISO/ IEC 15946-2-2002, (Information Technology, Security techniques, Cryptographic techniques based on elliptic curves) Part 2: Digital Signatures, 2002
[11]. ISO/ IEC 15946-3-2002, (Information Technology, Security techniques, Cryptographic techniques based on elliptic curves) Part 3: Key Establishment, 2002.
[12]. ISO/ IEC 14888-3-2006, (Information Technology, Security techniques, Digital Signatures with appendix) Part 3: Discrete logarithm based Mechanisms, 2006.
[13]. ANSI X9.63. Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2001.
[14]. IEEE P1363, Standard Specifications for Public Key Cryptography, 2000.
[15]. Lang, Serge, "Elliptic curve: Diophantine Analysis", Springer-Verlag, New York, 1978.
[16]. N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, vol. 48, Pages 203–209, 1987.
[17]. V. S. Miller, "Use of elliptic curves in cryptography", in CRYPTO '85: Proceedings of the Advances in cryptology, vol. 218 of Lecture notes in computer sciences, (New York, NY, USA),Pages 417–426, Springer Verlag New York, Inc., 1986.
[18]. Hankerson, D., Menezes, A. and S. Vanstone, "Guide to Elliptic Curve Cryptography", 1st edition, Springer, ISBN-13: 978-0387952734, 2004.
[19]. L. Batina, S. B. Örs, B. Preneel, and J. Vandewalle, "Hardware architectures for public key cryptography", Integration, the VLSI Journal, vol. 34, Pages 1–64, 2003.
[20]. N. Nguyen, K. Gaj, D. Caliga, and T. El-Ghazawi, "Implementation of elliptic curve cryptosystems on a reconfigurable computer", Proceedings of IEEE Field Programmable Technology, Pages 60–67, 2003.