ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

A Survey Report on Elliptic Curve Cryptography

[1] Ajit Karki
[1] MTech, Assistant professor. Dept. Of Computer Science, The ICFAI University, Sikkim.

Abstract - **Information is an asset that has a value like any other asset. As an asset, information needs to be secured from attacks. To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (availability).During the last three decades, Computer networks created a revolution in the use of information. Information is now distributed. Authorized people can send and receive information from a distance using computer networks. Although the three above mentioned requirements- confidentiality, integrity, and availability- have not changed, they now have some new dimensions. Not only should information be confidential when it is stored; there should also be a way to maintain its confidentiality when it is transmitted from one computer to another. The scorching enlargement in the use of mobile and wireless devices demands a new generation of Public Key Cryptography schemes that has to accommodate limitations on power and bandwidth, at the same time, to provide an ample level of security for such devices. Elliptic Curve Cryptography (ECC) is rising as an attractive public-key cryptosystem for mobile/wireless environments. Compared to long-established cryptosystems like RSA, ECC offers the same security with smaller key sizes, which results in faster computations; lower power consumption, as well as memory and bandwidth savings. This is particularly useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity. Nevertheless, the true crash of any public-key cryptosystem can only be evaluated in the context of a security protocol. Elliptic Curve Cryptography (ECC) has become the ideal choice for the insidious computing environment because of its suitability to the devices having limited bandwidth, battery power, less computational resources and less memory.**

Keywords: **Cryptography, ECC, Integrity, Authentication.**

1. CRYPTOGRAPHY

It is a base of the modern electronic security technologies which is used to keep valuable information wherewithal on intranets, extranets, and the Internet so that cryptography is the indispensable science of providing security for information.

1.1 Objectives of Cryptography

The purpose of cryptography is providing security to shield information resources by making unauthorized acquirement of the information or tampering with the information more costly than the latent value that might be gained. Because the value of information usually decreases over time, good cryptography based security mechanism to shield information until its value is considerably less than the cost of unlawful attempts to obtain or tamper with the information. Good cryptography, when properly implemented and used, makes attempts to violate security cost-prohibitive. Another objective of all information security systems, including cryptography-based mechanism security systems are to protect information resources at less cost than the value of the information that is being protected.

1.1.1 Choice of Public Key Cryptosystem

When it comes to choosing which public key cryptosystem to use in a mobile environment, one has to keep in mind limitations on bandwidth, memory and battery life. In constrained environments such as mobile phones, wireless pagers or PDAs, these resources are highly limited. Thus, a suitable public key scheme would be one that is efficient in terms of computing costs and key sizes. Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the secure communication basically have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations for communication. Only the particular user knows the private key whereas the public key is distributed to all users or device taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices or users taking part in the communication and domain parameters in ECC are the example of such constants. Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but it is much slower than the private key cryptography.

Today, the ECC has the highest strength-per-bit compared to other public key cryptosystems. Small key sizes translate into savings in bandwidth, memory and processing power. This makes ECC the obvious choice in this situation. However, there are other aspects that need to be taken into account. In the following section, we will examine the different mathematical problems that underlie the majority of the public key cryptosystems in use today. This will give us a better understanding of the security on which different types of public key cryptosystems are based.

2. INTRODUCTION TO ECC

Security is one of the most important parts of the modern computer science. The Internet today is a truly global marketplace, with a wide variety of goods and services available online. Secure communication is an inherent requirement for many popular online transactions such as e-commerce, stock trading and banking. With the rapid deployment of applications like online banking, stock trading and corporate remote access, recent years have seen an explosive growth in the amount of sensitive data exchanged over the Internet. These transactions employ a combination of public-key and symmetric-key cryptography to authenticate participants and guarantee the integrity and confidentiality of information in transit. RSA Cryptography and Elliptic Curve Cryptography are the public key cryptography systems which are used these days. After two decades of research and development, elliptic curve cryptography (ECC) [1] has now gained widespread coverage and acceptance, and has ultimately moved from being an interesting mathematical construction to a well-established public-key cryptosystem already included in numerous standards and adopted by an increasing number of companies. In fact, ECC is no longer new, and has withstood in the last years a great deal of cryptanalysis and a long series of attacks, which makes it appear as a mature and robust cryptosystem at present.

Proposed independently by Neal Koblitz and Victor Miller in 1985, elliptic curve cryptography (ECC) has the special characteristic that to date, the best known algorithm that solves it runs in full exponential time. Its security comes from the elliptic curve logarithm, which is the DLP in a group defined by points on an elliptic curve over a finite field. This result in a dramatic decrease in key size needed to achieve the same level of security offered in conventional PKC schemes.

The idea that technology is moving beyond the personal computer to everyday devices with embedded technology and connectivity, as computing devices become progressively smaller and more powerful, is called ubiquitous computing or pervasive computing. It is the result of computer technology advancing at an exponential speed. Pervasive computing goes beyond the realm of personal computers: it is the idea that almost any device, from clothing to tools, appliances, cars, homes, human body and even your coffee mug, can be embedded with chips to connect the device to an infinite network of other devices. The goal of pervasive computing, which combines current network technologies with wireless computing, voice recognition, Internet capability and artificial intelligence, is to create an environment where the connectivity of devices is embedded in such a way that the connectivity is inconspicuous and always available.

Many of these devices require secure connections to each other, to ensure that the information they provide remains confidential, and that only those authorized to control these devices can do so. Providing security in such environment will be a critical task because the devices used are too modest to handle heavyweight security algorithms like RSA, DES etc. Until now, almost every type of wireless device like sensor nodes, cell phones, PDAs, Ad-hoc networking devices etc. have been provided security through these algorithms. ECC is emerging as an attractive public-key cryptosystem for mobile/wireless environments. Compared to traditional cryptosystems like RSA, ECC offers equivalent security with smaller key sizes, faster computation, lower power consumption, as well as memory and bandwidth savings. This is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity.

2.1Mathematical background of ECC:

An elliptic curve can be described as the set of solutions for the equation $y^2 \equiv x^3 + ax + b \pmod{p}$ where a, b є Zp such that $4a^3 + 27b^2$ # 0, including the point infinity O. The efficiency of elliptic curve algorithm is determined by various factors like selecting finite field (prime / binary), coordinate representations (Affine, Projective, Jacobian, Chudnovsky Jacobian and Modified Jacobian coordinate), elliptic curve arithmetic, scalar representation etc.

The underlying hard problem of ECC is the intractability of the elliptic curve discrete logarithm problem (ECDLP). As no sub-exponential algorithms are known to solve a generic instance of this problem, the key sizes are allowed to be much smaller than other public key cryptosystems like RSA.

The locus of a point, whose coordinates conform to a particular cubic equation along with the point at infinity O (the point at which the locus in the projective plane

intersects the line at infinity,) is known as an elliptic curve. The equation of E (Fp) for the characteristic p > 3 can be defined as $y^2= x^3+ ax + b$
(2).
Where, a ∈ F_p and b ∈ F_p are constants such that $4a^3+ 27b^2 \neq 0$. In the binary case the defining equation of $E(F_2{}^m)$ can be written as: $y^2+ xy= x^3+ax^2+ b$
(2).
where a∈ F_2 and b ∈ $F_2{}^m$ are constants and b ≠ 0.

A collection of points can be formed with the aid of a chord -and-tangent rule (extended addition) in an elliptic curve E defined over the field K as denoted in Figure 1.

Using basic coordinate geometry and given two points $P_1=(x_1, y_1)$ and $P_2=(x_2, y_2)$, one constructs arithmetic to compute the point $P_3=(x_3, y_3)=P_1+P_2$ as follows:
$x_{3}=\lambda^2-x_1-x^2$ (3)
$y_3=\lambda(x_1-x_3)-y_1$ (4)

where
λ={(Y2-Y1)/(x2-x1), if P1 ≠P2
(3X12+a)/(2y1), otherwise

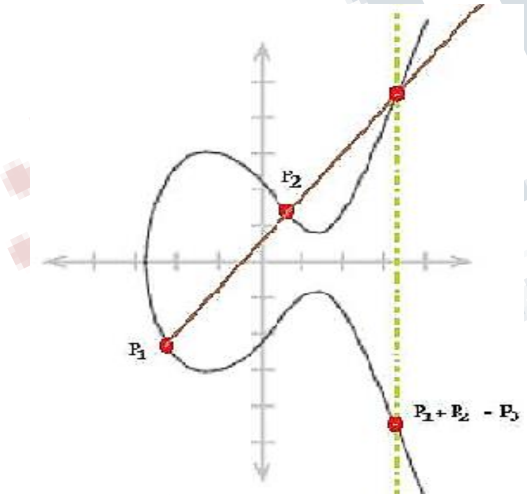

Figure 1: Addition of two elliptic curve points [1].

Let $P_1$and P_2 be two distinct points and let them intersect the elliptic curve in a straight line, then the straight line will bear a third intersection with the curve. The sum of P_1 and P_2, represented as P_3, is obtained as the reflection of the third intersection on the x axis. An Abelian group [3] is created with the set of points defined by the extended addition extended by the point ∞.

The Elliptic Curve Discrete Logarithm Problem can be stated as follows:

Given an elliptic curve E defined over GF(q), and two points P,Q E, find an integer x such that Q = xP, if such x exists. The security of ECC depends on the difficulty in solving the ECDLP. Solving the ECDLP is harder than solving both, the integer factorization problem (IFP), as well as the discrete logarithm problem (DLP) [4].

2.2 Elliptic curve domain parameters:

Two types of elliptic curve domain parameters may be used: elliptic curve domain parameters over **Fp** and elliptic curve domain parameters over **F_2 m**. ECC uses modular arithmetic or polynomial arithmetic for its operations depending on the field chosen.

2.2.1 Parameters over Fp:

The domain parameters for Elliptic curve over Fp are *p, a, b, G, n* and *h*, where *p* is the prime number defined for finite field Fp , *a and b* are the parameters defining the curve *y^2 mod p= x3 + ax + b mod p* , *G* is the generator point (xG, yG), *n* is the order of the elliptic curve. The scalar for point multiplication is chosen as a number between 0 and *n – 1, h* is the cofactor where *h = #E(Fp)/n* , *#E(Fp)* is the number of points on an elliptic curve.

2.2.2 Parameters over F2m:

The domain parameters for elliptic curve over F_2*m* are *m, f(x), a, b, G, n and h,* where *m* is an integer defined for finite field F_2*m*. The elements of the finite field F_2*m* are integers of length at most m bits, *f(x)* is the irreducible polynomial of degree m used for elliptic curve operations, *a* and *b* are the parameters defining the curve $y^2 + xy = x^3 + ax^2 + b$, *G* is the generator point *(xG, yG)*, a point on the elliptic curve chosen for cryptographic operations, *n* is the order of the elliptic curve. The scalar for point multiplication is chosen as a number between *0* and *n – 1*, *h* is the cofactor where *h = #E (F2m)/n*, *#E (F_2m)* is the number of points on an elliptic curve.

3. ECC vs. CONVENTIONAL CRYPTOSYSTEMS:

The most important fact that sets ECC ahead of other conventional cryptosystems is that for a well chosen elliptic curve, the best method currently known for solving the ECDLP is fully exponential, while sub exponential algorithms exist for other conventional cryptosystems. This difference means that ECC keys have much fewer bits than IFP and DLP based applications. It also causes a large difference in their running times. The relative computational performance advantage of ECC versus RSA is not indicated by the key sizes but by the cube of the key sizes. The difference becomes even more dramatic as an increase in RSA key size leads to an even greater increase in Computational cost. So, moving from 1024-bit RSA key to 3072-bit RSA key requires about 27 times (3^3) as much computation while ECC would only increase the computational cost by just over four times (1.63).The ratio of 256-bit ECC to 3072-bit RSA security level has already been increased to a value between 20 and 60, depending on optimizations. To secure a 256-bit AES key, ECC -521 can be expected to be, on an average, 400 times faster than 15,360-bit RSA.ECC is best suited in constrained environments. The advantages like speed and smaller keys or certificates are especially important in environments where at least one of the following resources is limited [4]: processing power, storage space, bandwidth, or power consumption.ECC uses smaller key sizes compared to traditionally used RSA based cryptosystems. Elliptic Curve Cryptography is especially suited to smart card based message authentication because of its smaller memory and computational power requirements than public key cryptosystems. It is observed that the performance of ECC based approach is significantly better than RSA and DSA/DH based approaches because of the low memory and computational requirements, smaller key size, low power and timing consumptions.

3.1 The ECC Advantage:

Much like the RSA challenge, the Certicom 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 [5]. 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 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. This difference largely contributes to the huge disparity in their respective running times. It also means that ECC keys have much fewer bits than IFP and DLP based applications. 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. While this deduction might be true, we have no way of proving it. We do not know if a fast and efficient elliptic curve DL algorithm that runs in sub-exponential time will be discovered, say, in the next ten years, or if another class of weak curves will be identified that could compromise the

Security of elliptic curve cryptosystems. But one thing is certain, after years of rigorous study, there is currently no faster way to attack the ECDLP other than fully exponential algorithms.

3.2 ECC Applications:

When the ECC was first introduced in 1985, there was a lot of uncertainty about its security. However, ECC has since come a long way. After nearly a decade of serious study and scrutiny, ECC has yielded highly efficient and secure. Presently, many product vendors have incorporated ECC in their products, and this number has only been on the rise. Uncertainty still exists among some proponents of traditional cryptographic systems, but they are starting to become more accepting of this promising new technology. RSA Security, for example, has long voiced concern regarding the security of ECC since its introduction. In recent years, however, RSA Security has researched on efficient ECC algorithms, and even acquired a patent on a storage-efficient basis conversion algorithm. Moreover, it has also integrated ECC into some of it's a product, acknowledging the fact that ECC has begun to establish itself as both secure and efficient.

4. ECC in PERSISTENT COMPUTING:

This section discusses the use of ECC in various fields that are important parts of persistent computing.

4.1 PC's:

Although devices having fewer resources are considered suitable for ECC, some companies are developing ECC based software to provide security on PCs, mainly for protection of data and for mail encryption. One such company is Guardian Edge Technologies, whose Data Protection Platform supports ECC. Its component products, Guardian Edge Hard Disk Encryption, Guardian Edge Removable Storage Encryption etc., use ECC with a 233-bit encryption key to protect critical data on a Windows based PC [9]. The Top Secret Messenger software was developed by Encryption Software Inc. It encrypts the messages of some of the most popular instant messaging programs today, like ICQ and MSN. It can also be used with e-mail clients such as Microsoft Outlook and Outlook Express to encrypt e-mail messages. This product uses both private and public key cryptosystems, including a 307-bit key for its implementation of the ECC [10].

4.2 Handheld and other small devices:

With omnipresent computing, we come across several devices such as PDAs, cell phones, home appliances, scientific instruments, and even medical devices such as pacemakers, which perform data collection and control functions using networking technologies [11]. These devices have limited computational resources and hence are ideal choices for the use of ECC. M-commerce using PDAs or mobile phones, requires a very high level of security. The security of m-commerce depends on the underlying PKC functions to provide authentication, integrity, non-repudiation and encryption. PDAs are considered to be a very popular choice for implementing public key cryptosystems because they have more computing power compared to most of the other mobile devices, like cell phones or pagers. The constantly increasing security requirements lead to an increased key size, which is a major problem for small devices. In such cases, ECC would definitely be a better choice [9].

4.3. Biometric Signature Verification:

An approach using biometric signatures, based on the ECC is proposed in [13]. The use of ECC in biometric signature creation improves the electronic banking security, as the public and private keys are created without storing and transmitting any private information anywhere. A secret key is to be shared between two parties through an insecure channel in symmetric cryptography. ECDH (Elliptic Curve Diffie –Hellman) is a protocol to create and share secret keys between parties without transmitting any private value, so no one has access to these secret keys except themselves. The mechanism detailed in [14], uses the ECC algorithm to agree on the domain parameters and to create the parties‟ private keys. By combining biometrics and the ECDH algorithm, secret messages can be generated in symmetric cryptography with help of dynamically generated private keys.

4.4 Bitcoin:

The crypto currency Bitcoin is a distributed peer-to-peer digital currency which allows “online payments to be sent directly from one party to another without going through a Financial institution” .The public Bitcoin block chain is a journal of all the transactions ever executed. Each block in this journal contains the SHA-256 hash of the previous block, hereby chaining the blocks together starting from the so-called genesis block. In Bitcoin, an Elliptic Curve Digital Signal Algorithm (ECDSA) private key serves as a user’s account. Transferring ownership of bitcoins from user A to user B is realized by attaching a digital signature (using user A’s private key) of the hash of the previous transaction and information about the public key of user B at the end of a new transaction. The signature can be verified with the help of user A’s public key from the previous transaction.

5. ECC IMPLEMENTATION:

ECC can be implemented in software and hardware [14]. Software ECC implementation provide moderate speed, higher power consumption and also have very limited physical security with respect to key storage. Where as hardware implementation improves performance in terms of flexibility. Also hardware implementation provides greater security since they cannot be easily modified or read by an outside attacker. Specified an approach to combine the advantages of software and hardware in new paradigm of computation referred as reconfigurable computing.

5.2 Mapping Methodology

The alphanumeric characters are mapped on to the points of the elliptic curve in the following methods.

5.2.1. Static (one-to-one) Mapping Method

From the cubic equation of Elliptic curve, for each given value of x, there are two values for y. One of these values of y and corresponding x will be used to map the any alphanumeric character. Like this, all numeric characters are mapped on to the different the x coordinates and their corresponding y coordinates of the given curve. Once the mapping of the all-alphanumeric characters onto the curve is completed, these points are encoded by using Elliptic curve Encryption techniques, which are transmitted through an insecure channel. The message is retrieved from the encoded data by using the Elliptic Curve decryption technique. The main advantage of this mapping methodology is simple. But the disadvantage is that the same alphanumeric characters from the different words are always mapped onto the same x-y coordinates of the elliptic curve points. When these points are encrypted, again these encrypted points are also the same, which are being transmitted through the insecure channel.

So, an intruder can easily interpret data with a trial and error method.
Since the alpha numeric characters are mapped on to the curve on basis of one-to-one, it is also easy for him to guess which character is mapped to which coordinate of the curve. Therefore secrecy of data transmission by using this methodology is very low.

5.2.2. Dynamic (One-to-N) Mapping Methods

In this method, alphanumerical characters are mapped on to the points of the Elliptic curve dynamically. For every transmission of the message from source to destination, the alpha-numeric characters mapping mechanism changed dynamically. For the every transmission of the message the mapping, encrypted, decrypted points are different. For an intruder it would be very difficult to guess on which points the alpha-numeric characters are mapped. Further, it is also difficult to guess which particular character is mapped to which point on the Elliptic Curve. Dynamic mapping method can strengthens the elliptic curve cryptosystem.

6. CONCLUSION:

Although ECC is a promising entrant for public key cryptosystem, its security has not been completely evaluated. The ECC has been shown to have many advantages due to its ability to provide the same level of security as RSA yet using shorter keys. Implementing ECC with the combination of software and hardware is advantages as it provides flexibility and good performance. Its disadvantage is its lack of maturity, as mathematicians believe that not enough research has been done in ECDLP. In particular, isogenies can be used as a one way function that can be used in these cryptographic primitives. However, this is now a deep and popular area of research. Also it has been found that hyper elliptic curves of higher genus are potentially insecure from a cryptographic point of view [14], yet the researchers are trying to prove it better than ECC. Elliptic curve Cryptography authentication scheme offers considerably greater data security for a given key size. If the key size is smaller it is also possible to implement for a given level of security so that it consume less power and less heat production. The smaller key size makes faster cryptographic operations, running on smaller chip and on more compact software. So for data security ECC is the great choice for following reason:

1. ECC provides great security of given key size.

2. By using smaller keys it make more compact implementation, fast cryptographic operations.

3. Less heat production and less power consumption.

4.In ECC, there is efficient and compact hardware implementation.

5. It is practically impossible to find private key so it is not possible for third party to obtain the secret.

7. REFERENCES:

[1] N.Koblitz, "Elliptic curve cryptosystems, in Mathematics of Computation,"1987, 203-209.

[2] V.Miller, "Use of elliptic curves in cryptography", Crypto 85, 5.

[3] L.Uhsadel, A. Poschmann and C.Paar, "An Efficient General Purpose Elliptic Curve Cryptography," In ECRYPT Workshop, SPEED-Software Performance Enhancement for Encryption and Decryption,2007, 95-104.

[4] Vanstone, S.A., "Next generation security for wireless: elliptic curve cryptography", Elsevier „Computers and Security", Vol. 22, No. 5, July 2003, 412-415.

[5] C. Coarfa, P. Druschel and D. Wallach, "Performance Analysis of TLS Web Servers", Network and Distributed Systems Security Symposium "02, San Diego,California, Feb.2002.

[6] Sun Microsystems Inc., "Speeding up Secure Web Transactions Using Elliptic Curve Cryptography", see http://research.sun.com/projects/crypto.

[7] Vipul Gupta, Douglas Stebila, and S.C. Shantz, "Integrating Elliptic Curve Cryptography into the Web"s Security Infrastructure" WWW2004, May 17–22, 2004 .

[8] Ganesh Ramakrishnan, CISA, "Secure Electronic Transaction (SET) Protocol (Or How to Transact Safely on the Internet)" Information Systems Control Journal, Vol. 6,2000.

[9] Byung kwan, Lee, Tai-Chi Lee and Seung Hae Yang, "An ASEP (Advanced Secure Electronic Payment) Protocol Design Using 3BC and ECC(F2m) Algorithm",

Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (IEEE‟04)

[10] Gianluigi Me and Maurizio A. Strangio, Proceedings of the Third International Conference on Information Technology and Applications (ICITA‟05), IEEE, 2005.
[11] Guardian Edge Technologies, A technical White Paper,December 05, available [online] at www.guardianedge.com.

[12] Xu Huang, Pritam Shah, and Dharmendra Sharma, “Fast Algorithm in ECC for Wireless Sensor Network”, IMECS 2010, Hong Kong, 2010.

[13] Shahriar Mohammadi and Sanaz Abedi, “ECC-Based Biometric Signature: A New Approach in Electronic Banking Security” International Symposium on Electronic Commerce and Security, IEEE, 2008.

[14] Sheikh Iqbal Ahamed, Farzana Rahman and Md. Endadul Hoque,““‟ ERAP: ECC based RFID Authentication Protocol”, IEEE 2008.