Application of Elliptic Curves in Designing Lightweight Cryptographic Techniques

Reema Jain
Department of Mathematics
Vivekananda Global University Jaipur
Email- jain.reema@vgu.ac.in

Received 27 January 2016, received in revised form 3 March 2016, accepted 3 March 2016

Abstract: **Besides the traditional computing environment now a day's Ubiquitous Computing has evolved. Ubiquitous Computing also known as pervasive computing is an advanced computing concept where computing is made to appear everywhere and anywhere. Ubiquitous computing can occur using any device, in any location, and in any format in which a user interacts with the computer, which can exist in many different forms, including laptop computers, tablets, terminals and phones. Furthermore there are applications in which devices have restricted processing capabilities, memory capacities, bandwidth support, power consumption, software support. Also the processing environment is so heterogeneous that predicting any behavior of any device may seem unfeasible. Security is an important issue in Ubiquitous Computing environment due to the heterogeneity of devices used in communication. Currently Elliptic Curve based cryptographic solutions have revolutionized the arena of security. The Elliptic Curve based solutions are usually based on difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). The Elliptic Curve based systems can attain to a desired security level with significantly smaller size keys than that of required by other public key cryptographic schemes. Using of Elliptic Curves we can make Light Weight Cryptographic Schemes for ubiquitous computing environment, which can be applied to the lower computational power devices, like smart card based applications, e-applications, mobile applications and many more, due to their lower computational cost and communication overhead. This paper elaborates the use of Elliptic Curves in designing Light Weight Cryptographic Techniques which are suitable for resource constrained devices at the same time providing all the security attributes like message confidentiality, authentication, integrity, unforgeability and non-repudiation, along with encrypted message authentication and forward secrecy of message confidentiality.**

Keywords: **Elliptic Curve, Elliptic Curve Discrete Logarithm Problem, Lightweight Cryptography.**

1. INTRODUCTION

The extended use of computer networks for information transmission and management, as well as the fact that the number of IT-users is increasing day by day, requires the role of security mechanisms. Security is an essential feature in almost all area of communication. While sending a message to a person over an insecure channel such as internet we must provide confidentiality, integrity, authenticity and non-repudiation. These are the four major security aspects [7] or goals for any system. To achieve these goals we can use either symmetric key cryptography or asymmetric key cryptography. Standard algorithms like DES, AES and RSA stood resistant towards linear, differential and algebraic attacks despite of a few reduced round attacks. It will be of great help towards security point of view if we could use such algorithms in a pervasive computing environment. But, we are well aware that pervasive devices have restricted capabilities in terms of memory storage, computational capabilities, power consumption and all. Restricted computational capability and memory storage limits implementation of traditional cryptographic algorithms in pervasive environment [1]. This may result even in compromise of the security of a pervasive environment. The solution to above issue is to design Lightweight Cryptographic Techniques[2] which can be easily implemented with the applications involving resource constrained devices. Light weight cryptography plays an important role in pervasive computing to deal with the security issues.

2. LIGHTWEIGHT CRYPTOGRAPHY

Lightweight cryptography is a relatively new field aimed to develop more efficient cryptographic implementations in response to typical constraints in the hardware used in ubiquitous computing environment [5]. The hardware used in ubiquitous or pervasive computing environment will likely be constrained in computational power, battery, as well as memory. Lightweight cryptography is tailored for such constrained devices, with the goal of balancing the tradeoffs between low resource requirements, performance, and cryptographic strength.

Light Weight Cryptography is designed for constrained devices. These devices have constraints in terms of speed, processing, memory space, power consumption, area, energy, size etc. Example of constrained devices includes mobile phones, RFID tags, smart cards etc. Alex [11] refers light weight cryptography as that it is as light as feathers and in terms of security it is immensely strong.

Lightweight cryptography got its focus when deployed in pervasive computer systems, where traditional cryptographic algorithms were not found very useful option. The challenge is to design secure applications without any heavy weight

cryptography [12]. There is always a tradeoff between security, cost and performance in light weight cryptography. Light weight cryptography has to compromise a no. of parameters compared to traditional cryptography. For example, key length is reduced from 256 bits to 56 bits, no. of rounds that run in an encryption process is reduced from 48 to 16 and the mode of architecture shifts from parallel to serialized. Memory requirement is reduced from giga bytes to kilo bytes. Processing speed comes down from GHz to KHZ. All this is because of the restrictions that we have for pervasive devices and pervasive computing environment.

Lightweight cryptographic algorithms should have a short computing process because of their restricted area, and perform serialization operations as parallel processing so that they consume more power. Also, they should have a short processing time such that their energy consumption is saved and should support short output to reduce communication cost amongst the devices Axel Poschman [11] also suggests that this is not intended for all adversaries and it is not a substitution for traditional cryptographic techniques. Most light weight cryptographic implementations target towards application specific integrated circuits (ASICs).

But the important question is "How to design Lightweight Cryptographic Techniques" that fulfill all the above considerations.

3. MATHEMATICS OF ELLIPTIC CURVES

A. Elliptic curves over F_q

In 1985 Niel Koblitz and Victor Miller from the University of Washington proposed the elliptic curve cryptosystem [8]. Elliptic curves over finite fields appeared to be intractable and hence ElGamal encryption and signature schemes have natural counterparts on these curves. Elliptic curve can be defined over F_q and F_2^m [6.] For simplicity we will discuss only Elliptic curves over F_q.

A finite field is a set of elements that have a finite order (number of elements).The order of *Galois Feld (GF)* [3] is normally a prime number or a power of a prime number. An elliptic curve E over F_q is the set of all solutions (x, y) ϵ $F_q \times F_q$ to an equation called *Weierstrass equation*

$$y^2 = x^3 + ax + b$$

where a, b ϵ F_q and $4a^3 + 27b^2 \neq 0$, together with a special point ∞ called the point at infinity [6].

It is well known that E is an (additively written) abelian group with the point ∞ serving as its identity element. The rules for group addition are summarized below.

B. Addition Formulas for the Curve

There is a rule, called the chord-and-tangent rule, for adding two points on an elliptic curve $E(F_q)$ to give a third elliptic curve point. Together with this addition operation, the set of points $E(F_q)$ forms a group with ∞ serving as its identity. It is this group which is used in the construction of elliptic curve cryptosystems. The addition rule is best explained geometrically [6].

Let P(x_1, y_1) and Q(x_2, y_2) are the two points on the elliptic curve. Then the sum of P and Q is denoted by another point say R = (x_3, y_3) as it is shown in Figure 1.

Let P =(x_1, y_1) ϵ E, then -P = (x_1, -y_1). If Q = (x_2, y_2) ϵ E , $Q \neq -P$, then P + Q = (x_3, y_3), where

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda (x_1 - x_3) - y_1$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & Otherwise. \end{cases}$$

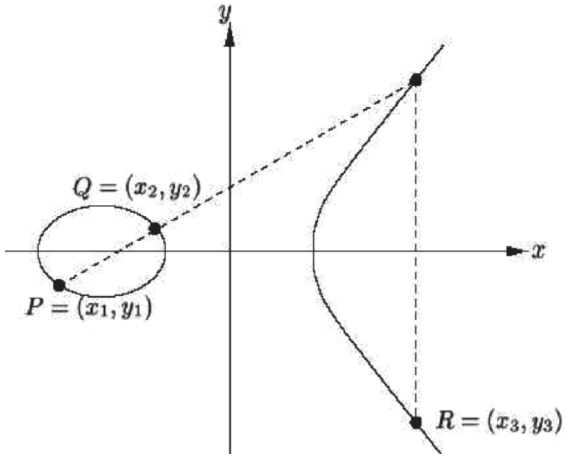

Figure 1: Addition of two points P and Q : R = P + Q [3]

The above elliptic curve is said to be non singular if it satisfy the following condition,

$$4a^3 + 27b^2 \neq 0$$

else, the curve is singular.

Doubling points on an elliptic curve C over GF(2^m) are defined in a similar way as shown in the Figure 2.

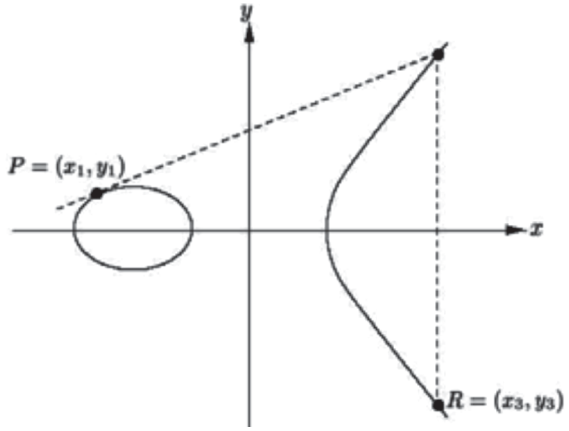

Figure 2: Doubling a point P : R=P+P=2P [3]

Excluding the point at infinity ∞, every point P = (x, y) on an elliptic curve C over GF(p^m) can be represented as (or "compressed" to) P = (x, y'),where y' is a single bit:

1. if x = 0 then y'=0.
2. if x $\neq$ 0, then y' is the parity of y when it is viewed as an integer.

An advantage of compressed representation of a point is that when a compressed point is stored internally in a computer or communicated over a network, it takes only one bit more than half of the bits required for storing or transmitting its uncompressed counterpart. This advantage, however, is not for free: recovering the y-coordinate from a compressed point involves a few arithmetic operations in the underlying finite field [8].

C. ECC Domain Parameters

Elliptic curve cryptography (ECC) [3] domain parameters over GF(P), can be represented by a six tuple:

E = (q, a, b, G, n, h), where

q = P or q = 2^m, where m is a natural number.

a and b are the coefficients of x^3 and x respectively used in the equation.

$$y^2 \equiv x^3 + ax + b \text{ (mod P) for q = P} \geqslant 3$$

$$y^2 + xy = x^3 + ax^2 + b \text{ for q} = 2^m \geqslant 1$$

G is a base point on the elliptic curve.

n is prime number which is of the order of G. The order of a point on an elliptic curve is the smallest positive integer r such that rP = ∞.

Finally h = |*E*| / n. where |*E*| represents the total number of points on elliptic curve and it is called the curve order.

D. ECC Key Generation

A public key Q = (x_q, y_q) associated with a domain parameter (q, a, b, G, n, h) is generated for an entity say *Alice* using the following procedure:

- Select a random number or pseudo random integer d in the interval [1, ..., n-1].
- Compute Q = dG.
- *Alice's* public key is Q and her private key is d.

4. ELLIPTIC CURVE BASED CRYPTOSYSTEM

Table 1 shows a comparison of key sizes of different cryptosystems. From this it is clear that ECC gives same level of security with a smaller key size as compare to others. But we must choose the ECC parameters carefully [10].

Table 1: A comparison of key sizes needed to achieve equivalent level of security with three different methods

Symmetric Encryption	**RSA and Diffe-Hellman**	**Elliptic Curve**
Key size in bits	Key size in bits	Key size in bits
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

An important advantage of elliptic curve is the shorter key lengths. ECC's unique properties make it especially well suited for resource constraint applications. It provides the highest strength per bit of any cryptosystem known today. Based on the best known algorithms today, one can estimate that 160-bit elliptic curves correspond to 1024-bit RSA, and 224-bit elliptic curves correspond to 2048-bit RSA (Table 1). Even though ECC was proposed in 1985 [8], the market was initially reluctant to move towards this new and more complex primitive. However, recently ECC has been adopted by the governments of Austria, Germany and the USA and is gaining more widespread acceptance. The main attraction lies clearly in the shorter key lengths, this advantage over RSA will increase over time. The EC-based approaches have a great computational advantage over their modular exponentiation-based counterparts when they are executed on constrained platforms. ECC also produces lightweight software implementations due to its memory and energy savings.

5. SECURITY ATTRIBUTES OF CRYPTOGRAPHIC TECHNIQUES BASED ON ELLIPTIC CURVE

The cryptographic technique based on elliptic curve cryptography provides the following security attributes. These attributes are based on the fact that it is almost intractable to solve the elliptic curve discrete logarithmic problem (ECDLP) [4, 8]. We should choose the parameters in such a way that it will become infeasible for an eavesdropper to solve ECDLP.

Confidentiality: The information will not be disclosed to any unauthorized individual or system.

Authentication: The identity of the message sender cab be verified without having the private key.

Integrity: The message cannot be altered in the communication.

Unforgeability: As we know Elliptic Curve Digital Signature Algorithm is unforgeable against adaptive attack. Hence it is unforgeable.

Non-repudiation: When dispute occurs between sender and recipient, the recipient can send the message to the judge for settling the original message M sent by the intended sender or not. Judge now run the verification algorithm and take the necessary action.

Forward Secrecy : An adversary that obtains private key of the sender will not be able to decrypt past messages.

Public Verification : Public verification function means that any third party can verify directly the signature of the sender of the original message without the sender's private key when dispute occurs.

Furthermore use of elliptic curve based cryptosystem solves the key exchange problem which is very important for many applications.

The security of Elliptic Curve Cryptosystem depends on how difficult it is to determine x given xP and P. This is referred to as the elliptic curve logarithm problem. The fastest known technique for taking the elliptic curve logarithm is known as the Pollard rho method. It has been seen that a considerably smaller key size can be used for ECC compared to RSA. Thus, there is a computational advantage to using ECC with a shorter key length than a comparably secure RSA [9]. The results show that ECC is efficient in terms of the size of Data files and Encrypted files.

6. CONCLUSION

Elliptic curve cryptography is the interesting area when it comes to less memory requirements and computational costs. ECC applied algorithms are of great use in environments where the level of security is medium and span of the security provision is less for example for a single session. From the above discussion it is clear that Elliptic Curve based Cryptosystems offers equal security for a far smaller key size, thereby reducing processing overhead and thus making the use of elliptic curve cryptography suitable in designing the light weight cryptographic techniques for pervasive or ubiquitous computing environment. Furthermore Elliptic Curve based techniques provide all the security attributes like message confidentiality, authentication, integrity and non-repudiation, along with encrypted message authentication and forward secrecy of message confidentiality and public verification. So, we can conclude that using Elliptic Curve based cryptosystems we can design the lightweight techniques which are suitable for pervasive devices and ubiquitous computing environment.

REFERENCES

[1] M.Satyanarayanan, Pervasive Computing: Vision and Challenges. *IEEE Personal Communications,* 2001.

[2] Paul C. van Oorschot Alfred J. Menezes and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[3] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. CRC Press, 2003.

[4] Behrouz A. Forouzan. *Cryptography and Network Security*. Tata McGraw-Hill, 2007.

[5] Rukma Rekha Prasad Babu. *International Journal on Computer Science and Engineering (IJCSE).* Vol. 4 No.2, 2012.

[6] Ram Shanmugam. *Elliptic curves and their applications to cryptography: An Introduction*. Andreas enge, Kluwer academic press, pages 164-168, 1999.

[7] William Stallings. *Cryptography and Network security: Principles and Practices*. Prentice Hall Inc., second edition, 1999.

[8] Scott A. Vanstone. *Elliptic curve cryptosystem the answer to strong, fast public-key cryptography for securing constrained environments.* Information Security Technical Report 2, pages 78 - 87, 1997.

[9] Mohsen Toorani and Ali Asghar Beheshti Shirazi. *LPKI - A Lightweight Public Key Infrastructure for the Mobile Environments*. Proceedings of the 11th IEEE International Conference on Communication Systems (IEEE ICCS'08), pp.162-166, 2008.

[10] William J Caelli, Edward P Dawson, and Scott A Rea. *Pki, elliptic curve cryptography and digital signatures.* Journal of Computers and Security, 18(1), pages 47 - 66, 1999.

[11] Thomas Eisenbarth, Sandeep Kumar, Christof Paar and Axel Poschmann, Leif Uhsadel. *A Survey of Lightweight-Cryptography Implementations.* IEEE Design & Test of Computers, November-December 2007.

[12] Munirul, Haque and Sheikh Iqbal Ahamed. *Security in Pervasive Computing: Current Status and Open Issues.* International Journal of Network Security, Vol.3, No.3, PP.203–214, Nov.2006.

◆ ◆ ◆