IJCAT International Journal of Computing and Technology, Volume 1, Issue 3, April 2014
ISSN : 2348 - 6090
www.IJCAT.org

Text Cryptosystem Based on Elliptic Curve Cryptography for Networks

[1] Akshay V. Fadnis, [2] S. U. Nimbhorkar

[1]Project Scholar, G. H. Raisoni College of Engineering
Nagpur (MS) India

[2]Assistant Professor,G. H. Raisoni College of Engineering
Nagpur (MS) India

Abstract - There is a rapid development in the area of Information Communication Technology. Mobile devices (e.g., PDA, mobile phone, and notebook PC) become necessary for a modern life. Users can use them to access many applications, for example online shopping, mobile pay TV, internet banking, which have been deployed on internet or wireless networks easily. Therefore, secure communications in such wireless environments are more and more important because that protects communication between users and servers from unlawful adversaries. Especially, users are people frail to attacks and there are many authentication schemes proposed to guarantee it. The Basic intension is to use mobile phones as nodes of M2M communications for IoT applications. By using elliptic curve algorithm in such a way that when algorithm ported onto mobile phones perform within limited speed limits and also consume less power consumption (light weight).

Keywords **- Identity Based Cryptography, Elliptic Curve Cryptography, M2M, IoT, Session Key.**

1. Introduction

The advent of E-Commerce demands for a secure communication of digital information. It has been proven for years that this can be achieved by cryptography. A set of cryptographic primitives used to provide information security services is generally referred to as a cryptosystem. The basic security services a cryptosystem should provide are Confidentiality, Integrity, Authentication, and Non-repudiation [2][3]. Confidentiality is keeping information secret from all other than those who are authorized to see it. Integrity is ensuring that the information has not been altered by unauthorized or unknown entities. Authentication is the assurance that the communicating party is the one that it claims to be. The corroboration of the identity of an entity is called Entity Authentication and corroborating the source of the information is called Message Authentication. Non-repudiation is preventing the denial of previous commitments or actions. Confidentiality can be achieved by a cryptographic primitive called Encryption. It is defined as a function which maps an intelligible plaintext to an unintelligible cipher text. Digital Signature is a fundamental cryptographic primitives which provides authentication, integrity and non-repudiation. The function of a digital signature is to provide a means for an creature to combine its identity to a portion of information. The process of signing entails converting the message and some covert information held by the entity into a mark called digital signature. Besides encryption and digital signature, Key Agreement is another fundamental cryptographic primitive for establishing a secure communication. It is a process of computing a shared secret contributed by two or more entities such that no single entity can predetermine the resulting value. An authenticated key agreement is attained by combining the key agreement protocol with digital signatures.

This avoids man-in-the-middle attack[4]. Symmetric key cryptosystems enable efficient encryption and some data integrity applications. Whereas asymmetric or Public Key Cryptosystems (PKC) enable efficient signature (particularly non-repudiation) and key management (which includes key agreement)[49]. In a traditional PKC, the association between a user's identity and his public key is obtained through a digital certificate issued by a Certifying Authority (CA). The CA checks the credentials of a user before issuing a certificate to him. If Alice wants to send a signed message to Bob, first she obtains a digital certificate for her public key from a CA. Alice then signs

a message using her private key and sends the signed message along with her certificate to Bob. Bob first identified the authority of the certificate by scrutiny the certificate revocation list available by the CA, then he identifies the signature using public key in the certificate. If many CAs are concerned between Alice and Bob the entire certificate lane has to be confirmed. Hence, the process of certificate management requires high computational and storage efforts [2]. To simplify the certificate management process, Shamir [3] introduced the concept of ID-based cryptosystem in 1984. In such cryptosystems the public key of a user is derived from his identity information and his private key is generated by a trusted third party called Private Key Generator (PKG). The advantage of ID-based cryptosystems is that it simplifies the key management process which is a heavy burden in the traditional certificate based cryptosystems. In these cryptosystems Alice can send an encrypted message to Bob by using Bob's identity information even before Bob obtains his private key from the PKG. In the case of signature Bob can verify Alice's signature just by using her identity information. In general, an identity based cryptosystem has the following properties:

– user's public key is his identity (or derived from identity).
– no requirement of public key directories
– message encryption and signature verification processes require only receivers' and signers' identity respectively along with some system parameters (params)1. These properties make ID-based cryptosystems advantageous over the traditional PKCs, as key distribution is far simplified. It needs a directory only for authenticated public system parameters of the PKG, which is clearly less burdensome than maintaining a public key directory for total users. However, they suffer from an inherent drawback of key escrow i.e. PKG knows the users' private keys. They also require a secure channel for key issuance between PKG and user. The ID-based cryptosystems require the users to authenticate themselves to their PKG in the same way as they would authenticate themselves to a CA in traditional PKC. Shamir[5], in his path breaking work, proposed an ID-based signature (IBS) scheme based on integer factorization problem.

Later, satisfactory and practical solutions for IBS schemes were proposed in [6, 7]. In ID-based PKC, everyone's public Keys are predetermined by information that uniquely identifies them, such as their email address. This concept was first proposed by Shamir [2]. Shamir's original motivation for ID-based encryption was to simplify certificate management in e-mail systems. Each entity in the system sends his/her identity to a trusted third party called the Key Generation Center (KGC), to obtain the private key. The private key is computed using the private key of the KGC and the identity of the user. Key escrow is inherent in ID-based systems since the KGC knows all the private keys. For various reasons, this makes implementation of the technology much easier, and delivers some added information security benefits. ID-based PKC (ID-PKC) remained a theoretical concept until [3] and [4] were proposed. Some of the issues to be addressed to compare the ID-based systems with the traditional PKI supported public-key cryptography.

2. Related Work

Elliptic Curve Cryptography (ECC) Domain Parameters

Elements of the ECC over a binary field are m-bit strings. The policy for arithmetic in binary field can be defined by either polynomial illustration or by optimal normal basis representation. Since binary field operates on bit strings, computers can do arithmetic in this field very proficiently. An elliptic curve with the underlying field over a binary field is formed by choosing the elements i and j within binary field (the only condition is that j is not 0). As a effect of the Binary field having a attribute 2, the elliptic curve equation is to some extent accustomed for binary illustration [14]:

$y^2 + xy = x^3 + ix^2 + j$

The elliptic curve includes all points (x, y) which persuade the elliptic curve equation over binary field (where x and y are elements of Binary Field). An elliptic curve group over Binary Field consists of the points on the equivalent elliptic curve, collectively with a point at infinity, O. There are finitely lot of points on such an elliptic curve.

As a very small example, consider the field $F_2$4 (f2m), defined by using polynomial illustration with the irreducible polynomial $f(x) = x^4 + x + 1$ [14].

The element g = (0010) is a generator for the field . The powers of g are:

g^0 = (0001) g^1 = (0010) g^2 = (0100) g^3 = (1000) g^4 = (0011) g^5 = (0110)

g^6 = (1100) g^7 = (1011) g^8 = (0101) g^9 = (1010) g^{10} = (0111) g^{11} =(1110)

g^{12} = (1111) g^{13} = (1101) g^{14} = (1001) g^{15} = (0001)
In a factual cryptographic application, the constraint m

must be large enough to prevent the efficient generation of such a table otherwise the cryptosystem can be busted. Nowadays, practice, m = 160 is a suitable choice. The table allows the use of generator details (g^e) rather than bit string notation, as used in the following example. Also, using generator notation allows multiplication without mention to the irreducible polynomial

$f(x) = x^4 + x + 1.$

Consider the elliptic curve $y^2 + xy = x^3 + g^4x^2 + 1$. Here a = g^4 and b = g^0 =1. The point (g^5, g^3) satisfies this equation over F_2m :

$y^2 + xy = x^3 + g^4x^2 + 1$

$(g^3)^2 + g^5g^3 = (g^5)^3 + g^4g^{10} + 1$

$g^6 + g^8 = g^{15} + g^{14} + 1$

(1100) + (0101) = (0001) + (1001) + (0001)

(1001) = (1001)

The fifteen points which satisfy this equation are:

(1, g^{13}) (g^3, g^{13}) (g^5, g^{11}) (g^6, g^{14}) (g^9, g^{13}) (g^{10}, g^8) (g^{12}, g^{12})

(1, g^6) (g^3, g^8) (g^5, g^3) (g^6, g^8) (g^9, g^{10}) (g^{10}, g) (g^{12}, 0) (0, 1)

These points are graphed below:

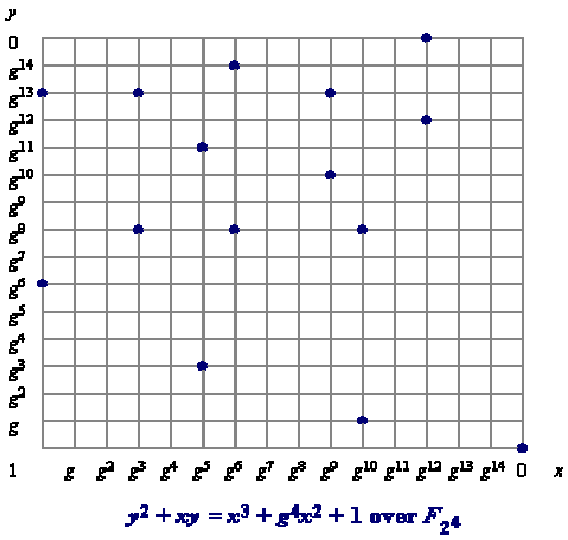

Figure1: Graph showing ECC Points

Elliptic curve groups over binary field have a set of number of points, and their mathematics involves no mistake. This united with the binary nature of the field, binary field arithmetic can be done very capably by a computer. The subsequent algebraic policies are applied for arithmetic over Binary field [14]:

Adding distinct points P and Q:

The downbeat of the point A = (xA, yA) is the point -A = (xA, xA + yA). If A and B are distinct points such that A is not -B, then

A + B = C where

s = (yA - yB) / (xA + xB)

$xC = s^2 + s + xA + xB + i$ and yC = s(xA + xC) + xC + yA

As with elliptic curve groups over real numbers, A + (-A) = O, the point at infinity. Furthermore, A + O = A for all points A in the elliptic curve group.

Doubling the point P:

If xA = 0, then 2A = O

Provided that xA is not 0,

2B = C where

s = xA + yA / xA

$xA = s^2 + s + i$ and $yC = xA^2 + (s + 1) * xC$

Recall that a is one of the attributes chosen with the elliptic curve and that s is the slope of the line all the way through A and B

Elliptic Curve Protocols:

Usually in the process of encryption and decryption, it has 2 entities, the one is encryption and the other is decryption.[8]. Let us assume that Alice is the person who is encrypting and Bob is the person decrypting. Alice's (or Bob's) public and private keys are linked with a particular set of elliptic key domain parameters (Q, FR, i, j, G, N, H).

Alice generates the public and private keys as follows

1. Select a random number D, D ∈ [1, N – 1]
2. Compare Q = dG.
3. Alice's public key is Q and private key is N.

It should be noted that the public key generated needs to be validated to ensure that it satisfies the arithmetic requirement of elliptic curve public key[11]. A public key Q = (a , b) associated with the domain parameters (Q, FR, i, ^{q}j, ^{q}G, N, H) is validated using the following procedure [12].

1. Check that $Q \neq O$
2. Check that a and b are properly represented elements of F
3. Check if Q lies on the elliptic curve defined by a and b.
4. Check that $NQ = O$

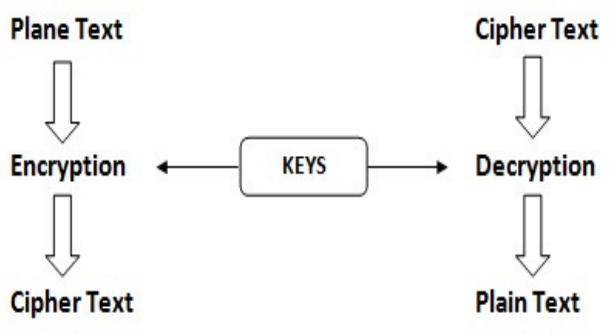

Figure2: Elliptic Curve Flowchart

From above Fig. any plaintext can be encrypted in a curve, image and other sources. For this purpose there is a need of private key to encrypt the plaintext to CipherText [9]. Similarly for decrypting CipherText to Plaintext enter the same key which was used for encrypting the text.

3. Conclusion

Implementation of Identity Based Cryptosystem using ECC provides better security. Every character in the message is shown by its ASCII value. Each of these ASCII value is converted into an affine point on the EC, by using a starting point called Pm. Conversion of the plaintext ASCII value by using an affine point is one of the aid of this work. The purpose of this Conversion is twofold. Firstly a single digit ASCII integer of the character is rehabilitated into a set of coordinates to fit the EC. Secondly the conversion introduces non-linearity in the character thereby completely camouflaging its uniqueness. This converted string of the message is encrypted by the ECC technique. Decryption of ECC encrypted message is itself quite a formidable task, unless this have knowledge about the private key 'NB' ,the secret integer 'k' and the affine point Pml.

References

[1] B S Adiga, Balamuralidhar P, Rajan M A, Ravishankara Shastry, Shivraj V L" *An Identity based Encryption using Elliptic Curve Cryptography for Secure M2M Communication*" ACM Journal IPICS 2012.

[2] Toan-Thinh TRUONG, Minh-Triet TRAN† & Anh-Duc DUONG "*Improvement of the more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on ECC*".IEEE Conference on Advanced Information Networking and Applications Workshops,OCT 2012

[3] Sonali Nimbhorkar, Dr.L.G.Malik "*Prospective Utilization of Elliptic Curve Cryptography for Security Enhancement*" International Journal of Application or Innovation in Engineering & Management Volume 2, Issue 1, January 2013.

[4] S. Maria Celestin Vigila , K. Muneeswaran" *Implementation of Text based Cryptosystem using Elliptic Curve Cryptography*".IEEE Trasaction on Advance Computing 2012

[5] Vermesan, O. Harrison, Vogt, M. , Kalaboukas, H.K., Tomasella , M. (Eds.), 2009. *The Internet of Things - Strategic Research Roadmap, Cluster of European Research* Projects on the Internet of Things, CERP-IoT, 2009.

[6] Dobkin, Daniel M. and Aboussouan, Bernard. 2009. Low Power Wi-Fi (IEE 802.11) for IP Smart Objects. Whitepaper, GainSpan Corporation, 2009.

[7] Aydos, M., Savas, E., and Koc, C. K. 1999. *Implementing Network Security Protocols based on Elliptic Curve Cryptography*. Proceedings of the Fourth Symposium on Computer Networks (Istanbul, Turkey, May 20-21, 1999).

[8] Standard specifications for public key cryptography, IEEE standard, pI363,2000.

[9] Williams Stallings, Cryptography and Network Security, Prentice Hall, 4 th Edition, 2000.

[10] Kevin M. Finnigin, Barry E. Mullins, Richard A. Raines, Henry B.Potoczny, "*Cryptanalysis of an elliptic curve cryptosystem for wireless sensor networks*," International journal ofsecurity and networks, Vol. 2, No. 3/4, pp. 260- 271,1999.

[11] Sangook Moon, "*A Binary Redundant Scalar Point Multiplication In Secure Elliptic Curve Cryptosystems,*" International journal of network security, Vol.3, No.2, PP.132-137, Sept. 1997.

[12] Jaewon Lee, Heeyoul Kim, Younho Lee, Seong-Min Hong, and Hyunsoo Yoon, "*Parallelized Scalar Multiplication on Elliptic Curves Defined over Optimal Extension Field,*" International journal of network security, VolA, No.1, PP.99- 106, Jan. 1995.

[13] Liu Yongliang, Wen Gao, Hongxun Yao, and Xinghua Yu , "*Elliptic Curve Cryptography Based Wireless Authentication Protocol,*" International journal ofnetwork security, VolA, No.1, PP.99-106, Jan. 1993.

[14]http://www.certicom.com