International Journal of Engineering Research and Technology.
ISSN 0974-3154 Volume 11, Number 4 (2018), pp. 615-619

http://www.irphouse.com

Cryptanalysis of an Improved ECDSA

Dhanashree K. Toradmalle[1], Jayabhaskar Muthukuru[2], B. Sathyanarayana[3]

[1]*Department of Computer Science and Engineering, K L E F, Vaddeswaram, India.*
[2]*Department of Computer Science and Engineering, K L E F, Vaddeswaram, India.*
[3]*Department of Computer Science & Technology, Sri Krishnadevaraya University, India.*

Abstract

Technology has become the fundamental tools these days. We have got technically inclined shoppers in every domain of the market today; be it education, travel, medicine, banking, shopping, recreation to call many. Every client desires service at their finger tips. Also, additionally to service the client nowadays isn't solely fascinated by practicality however conjointly demands believability that is one in every of the key factors of security. Non-repudiation is unacceptable in any dealing over the internet. The challenge to security is to strategies produce this acute demand to the client in resource forced environments at lower machine speed and price. Digital signatures are thus integral to each application that demands security of knowledge. The elliptic curve primarily based digital signature is associate degree economical technique of adding security to such applications. This paper discusses the weather of elliptic curve and its role in digital signature. The paper also discusses the varied ECDSA and their safety features. It additionally portrays the issues within the security side of the strategies.

Keywords: Digital Signature, Elliptic curve, Elliptic curve digital signature algorithm

I. Introduction

A 'signature' indicates approval of any activity. It is a driving factor for a secure communication. Signing has been a very traditional yet important phase of data transfer over a communication channel. Document signing has been a tedious task for decades. With the evolution of computers and immense data transfer and storage the traditional method of physically signing documents cannot withstand the high demands of security. Thus, digital signature plays a pivotal role over the internet in today's times.

A digital signature is an asymmetric public key algorithm used to approve a document digitally. It is completely message oriented and assures that the Sender takes responsibility for sending messages and cannot deny his involvement in the process. Also, the Receiver of the message validates it to ensure that the message is not tampered during transmission.

So digital signature is a strong contender in providing protection against threat and forgery. The noteworthy phases of a digital signature are:

1. A *domain parameter generation phase* that generates a set *D* of domain parameters required for Signature Analysis.
2. A *key generation phase* that takes the input from a set *D* of domain parameters and creates key pairs *(Q,x)*.
3. A *signature generation phase* that takes the input from a set of domain parameters *D*, a private key *x*, and a message *m*, and generates a signature.
4. A *signature verification phase* that takes the information as the domain parameters *D*, a public key *Q*, a message *m*, and a purported signature and recognizes or rejects the signature.

Since the digital signatures are widely accepted and believed it is important to direct the use of principles endorsed by the regulatory bodies in the field of cryptology. The NIST National Institute of Standards and Technology supports the three benchmarks [1]: Rivest Shamir and Adleman Algorithm (RSA), Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA).

I.I Elliptic Curves:

Neal Koblitz and Victor Miller [2][3]in 1985 independently proposed elliptic curves for designing public-key cryptographic systems. Elliptic curves provide security which is equivalent to classical systems using fewer bits [4].It is estimated in [5] that a RSA needs 4096 bits of key size as compared to 313 bits required by elliptic curve system to achieve the same level of security. It indicates that elliptic curve cryptosystems require smaller chip size, less power consumption etc,.

An elliptic curve is represented in many alternate forms [6]. The Weierstrass equation of an elliptic curve E over a field K is given as:

$y^2 = x^3 + ax + b$ where x is not a continuous point and a and b are constants.

I.II Arithmetic used in Elliptic curves:

Elliptic curve primarily works on the the arithmetic of points on its curve .The two key operations on the elliptic curve are [1]:

- Point Addition: It is a *chord-and-tangent rule* for adding two points P(x1,y1) and Q(x2,y2) in *an Elliptic curve* to generate a new third point R(x3,y3) on it i.e P + Q = R
- Point Doubling: When a tangent is drawn at a Point P(x1, y1) on the elliptic curve which when intersected at a second point P(x2, y2), gives a new reflected point R(x3, y3) at the X-axis. i.e P +P= R

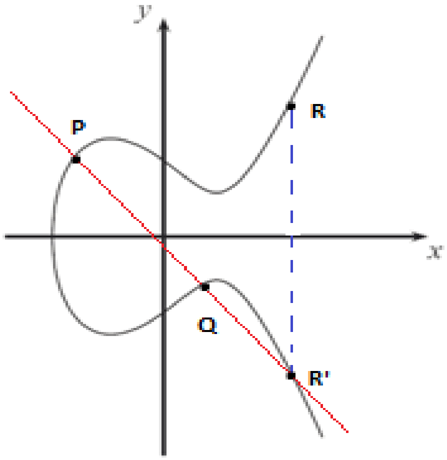

Fig 1. Point Addition in Elliptic Curve

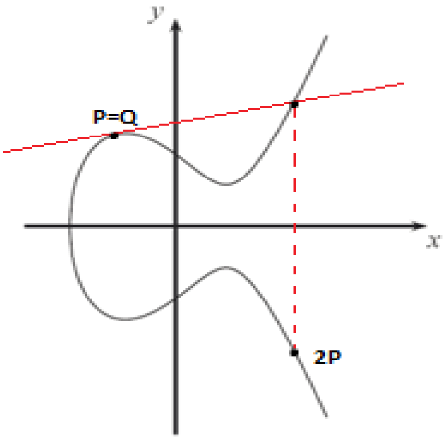

Fig 2. Point Doubling in Elliptic Curve

II. Cryptanalysis of Hong Zhong [7] et al Scheme:

Small key size and high security are the advantages *ECDSA* takes of *ECC*. Hong Jhong et al scheme proposed an improved method of ECDSA. The notations used are as follows:

G: Base point of elliptic curve

d: Private key of Alice

m: message

e: hash value of message m

Hong Jhong et al Signature Generation Method**:**

When Alice sends the message to Bob, and so obtains a digital signature *r*, *s* which is generated by following steps:

Step 1*:* Select a random k in the range of [1, n - 1].

Step 2: Compute a curve point k* G = (x1, y1)

Step 3: Compute value of r = x1 mod n. If r = 0, then go back to step 1

Step 4: Compute the value of e =SHA -1(m)

Step 5: Compute the value of s =(e +k + rd) mod n. If s=0, then return to step1

Step 6*:* Send the message *m* and computed digital signature (r, s)

Bob verifies the digital signature in following steps:

Step 1: Confirm that r and s are integers in [1, n-1].If not signature is Invalid.

Step 2: Ascertain e = SHA -1(m).

Step 3: Ascertain w = (s - e) mod n.

Step 4: Ascertain a curve X= w * G – r * Q =(x1, y1)

Step 5: On the off chance that If X=0, the digital signature is invalid else ascertain v=x1 mod n.

Step 6: Bob will acknowledge the digital signature if and only if *v* = *r*.

The Middle Man or intruder can without much of stretch modify or supersede the message that can't be perceived by the receiver, by merely adding the hash price. Let M1 be Middle Man‘s message, that is modified or supplanted the initial message m, having the hash values e1 and e severally. This attack is discussed below:

The attack is described as follows:

1. Calculate hash value e of the message m
2. Calculate signature for message m, *s =e +k +rd*
3. New/modified message m1
4. Calculate hash value e1 of the message m1
5. Calculate signature for new message m1, *s1= s - e + e1*
6. Signature for the message m1 is (s1, x1).

Substitute value of s from step 2 in step 5 we get, s1 = e + k + d – e + e1 where s1 is Middle Man’s signature element.So intruder can add new hash value and modify the message without knowing private or public key of the Sender and Receiver. This modification cannot be recognized by the receiver which is a threat to security.

III. Conclusion

The security of Hong Jhong’s scheme is analyzed during this paper, and it is found that it's one in all the foremost crucial flaw of Man in the Middle attack. The scheme tries to attain potency by reducing the reserve standard inverse operations however it fails to attain security; because the intruder will simply alter the message and replace the present message hash value with changed hash value and thereby it fails to attain security attributes of a digital signature sheme.

References

[1] Hankerson, A. Menezes, S. Vanstone. *Guide to Elliptic Curve Cryptography Springer 2004),* ISBN 0-387-95273-X.

[2] V. S. Miller, Use of Elliptic Curves in Cryptography *Springer- Verlag Berlin Heidelberg*, 1986.

[3] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation, vol. 48*, pp. 203-209, 1987.

[4] Lawerence C Washington, *Elliptic Curves Number Theory and Cryptograpy ©*, Taylor & Francis Group, LLC 2008

[5] I.F. Blake, G. Seroussi, and N.P Smart, Elliptic Curves in Cryptography, *Vol.265 of London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, *2000. Reprint of the 1999 original.*

[6] Samta Gajbhiye, Monisha Sharma, Samir Dashputre, A survey report on Elliptic curve Cryptography, *International Journal of Electrical and Computer Engineering (IJECE),Vol.1, No.2, December 2011*, pp. 195~201

[7] Hong Zhong, Rongwen Zhao, Jie Cui*, Xinghe Jiang and Jing Gao, An Improved ECDSA Scheme for Wireless Sensor Network, *International Journal of Future Generation Communication and Networking Vol. 9, No. 2* 2016, pp. 73-82.