International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-2, December 2013

A Secure Elliptic Curve Digital Signature Approach without Inversion

Jayabhaskar Muthukuru, B. Sathyanarayana

Abstract— The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA). Unlike the ordinary discrete logarithm problem elliptic curve discrete logarithm problem (ECDLP) has no sub-exponential time algorithm, due to this the strength per key bit is substantially greater when compare with conventional discrete logarithm systems. Elliptic curve based digital signatures are stronger and ideal for constrained environments like smart cards due to smaller bit size, thereby reducing processing overhead. Considering the security of data it is lacking regarding random number choosing or determination. This lacking leads to recovery of the private key in original Elliptic Curve Digital Signature scheme. This problem is overcome by our proposed digital signature scheme which is presented in this paper.

Index Terms— Digital Signature, ECDSA, Elliptic Curve Cryptography, Elliptic Curve Digital Signature Algorithm.

I. INTRODUCTION

A digital signature is a checksum which depends on the time period during which it was produced. It depends on all the bits of a transmitted message, and also on a secret key, but which can be checked without knowledge of the secret key. The Digital Signature Algorithm (DSA) was specified in a U.S. Government Federal Information Processing Standard (FIPS) called the Digital Signature Standard (DSS). Its security is based on the computational intractability of the discrete logarithm problem (DLP) in prime-order subgroups of Z*p At this time, there are three popular public-key algorithms which can provide digital signatures:

1. Elliptic Curve Digital Signature Algorithm (ECDSA) [1]
2. RSA scheme [2]
3. ElGamal signature scheme [3]

Among these ECDSA provides a faster alternative for public-key cryptography, much smaller key lengths are required to provide a desired level of security [1].

In 1985, the Elliptic Curve Discrete Logarithm Problem (ECDLP) was proposed independently as a new cryptographic scheme by koblitz [4] and Miller [5]. It is considered that the security of ECC is sufficiently proved. Since the ECDLP appears to be significantly harder than the DLP, the elliptic curve systems appears efficient than in conventional discrete logarithm systems.

Manuscript published on 30 December 2013.
* Correspondence Author (s)
Dr Jayabhaskar Muthukuru*, Department of Computer Science and Engineering, KL University, Vaddeswaram, Guntur, India.
Prof. B. Sathyanarayana, Department of Computer Science & Technology, Sri Krishnadevaraya University. Ananthapur, India.

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the DSA. ECDSA was first proposed by Vanstone in 1992[6] in response to NIST's (National Institute of Standards and Technology) request for public comments on their first proposal for DSS. It was accepted in 1999 as an ANSI standard, and was accepted in 2000 as IEEE PI363 [7] and NIST's FIPS 186-2 [8] standards. It was also accepted in 1998 as an ISO standard, and is under consideration for inclusion in some other ISO standards

II. OVERVIEW OF ELLIPTIC CURVE ARITHMETIC

Elliptic curve cryptosystems (ECC) were invented by Neal Koblitz [4] and Victor Miller [5] in 1985. The mathematical basis for the security of elliptic curve cryptosystems is the computational intractability of the elliptic curve discrete logarithm problem (ECDLP) [9].

An elliptic curve E over F_p is defined by an equation of the form:

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

where a, b $\in F_p$, and 4a3 + 27b2 $\neq$ 0 (mod p), together with a special point O, called the point at infinity. The set E(F_p) consists of all points (x, y), x$\in F_p$, y$\in F_p$, which satisfy the defining equation, together with O. We denote the curve by E(F_p).

Figures 1 and 2 show point addition and point doubling operations over an elliptic curve.

The basic EC operations are point addition and point doubling. Elliptic curve cryptographic primitives require scalar point multiplication. Say, given a point P(x, y) on an EC, one needs to compute kP, where k is a positive integer. This is achieved by a series of doubling and addition operations of P (see e.g [10]).

Definition of elliptic curve over F_P as follows [11].

Let p be a prime in F_P and a, b$\in F_P$ such that

$4a^3 + 27b^2 \neq 0$ mod p in F_P, then an elliptic curve E (F_P) is defined as

$$E(F_P) := \{ p(x, y), x, y \in F_P \}$$

Such that $y^2 = x^3 + ax + b$ mod p together with a point O. Below is the definition of addition of points P and Q on the elliptic curve E(F_P). Let P (x_1, y_1) and Q (x_2, y_2) then

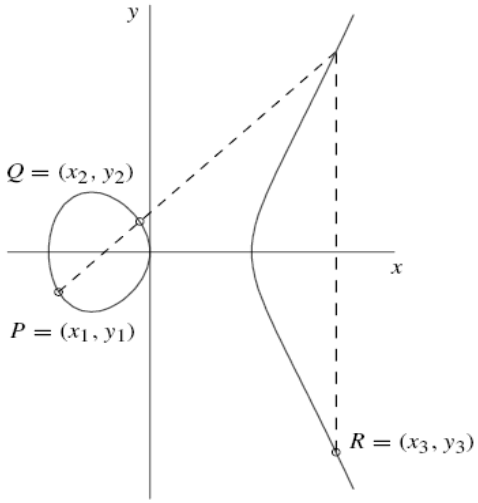

Fig.1. Addition: R=P+Q

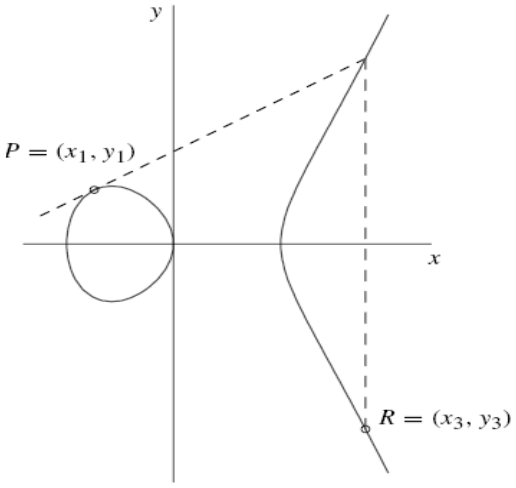

Fig.2. Doubling: R=P+P

$$R = P+Q = \begin{cases} O & \text{If } x_1 = x_2 \text{ and } y_2 = -y_1 \\ Q = Q+P & \text{If } P = O \\ (x_3, y_3) & \text{otherwise} \end{cases}$$

Where

$$x_3 = \begin{cases} \lambda^2 - x_1 - x_2 & \text{If } P \neq \pm Q \text{ (Point Addition)} \\ \lambda^2 - 2x_1 & \text{If } P = Q \text{ (Point Doubling)} \end{cases}$$

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

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{If } P \neq \pm Q \text{ (Point Addition)} \\ \dfrac{3x_1^2 + a}{2y_1} & \text{If } P = Q \text{ (Point Doubling)} \end{cases}$$

The point p(x, -y) is said to be the negation of p(x, y).

III. PROPOSED DIGITAL SIGNATURE BASED ON ELLIPTIC CURVE

In original ECDSA the private can be recovered if two different messages are signed by using same random number. To solve this problem, we proposed a new Digital Signature algorithm based on Elliptic Curve. Digital Signature scheme is developed without modular inversion operation in Signature generation and Verification algorithms. Proposed scheme signature contained three elements and the scheme consists of following three phases.

- Key pair generation
- Signature Generation
- Signature Verification

Notations:

To be convenient in description of our work the attributes are defined as

d : private key
Q : Public key
m : message
H() : a secure one-way hash function
r, s_1, s_2 : Signature elements
q: field order
FR: field representation
a, b: coefficients
G: base point
n: Order of G
h: co-factor

Key pair d and Q generated by the Signer as follows

Key pair Generation Algorithm:

INPUT: D= (q, FR, a, b, G, n, h)
OUTPUT: Q, d
Select d ∈ [1,….,n-1]
Compute Q = dG
Return (Q, d)

Message m can be signed by the signer as follows.

Signature Generation Algorithm:

INPUT: D= (q, FR, a, b, G, n, h), d, m
OUTPUT: Signature (r, s_1, s_2)
Begin
repeat
k = Random[1,2,…. , n-1]
P = kG
c = X-Co-ordinate(P)
e = H(m) mod n
s_1 = ec mod n
s_2 = (dc + k) mod n
R = eP
r = X-Co-ordinate(R)
until r ≠ 0 and s_1 ≠ 0 and s_2 ≠ 0
return (r, s_1, s_2)
End

To verify the signature (r, s_1, s_2) on message m, receiver does the following:

Signature Verification Algorithm:

INPUT: D= (q, FR, a, b, G, n, h), Q, m, Signature (r, s_1, s_2)
OUTPUT: Acceptance or rejection of the signature.

Begin
  if r, s_1, $s_2 \notin [1,\ldots, n-1]$ **then**
    Return ("Reject the signature")
  end if
  e = H(m)
  t = es_2
  U_1 = tG
  U_2 = s_1Q
  W = $U_1 - U_2$
  v = X-Co-ordinate(W)
  if v = r **then**
    Return ("Accept the signature")
  else
    Return ("Reject the signature")
  end if
End

IV. PERFORMANCE COMPARISON

We implemented original ECDSA and our proposed scheme and compared their performance over Elliptic Curve P-160 and presented the results below.

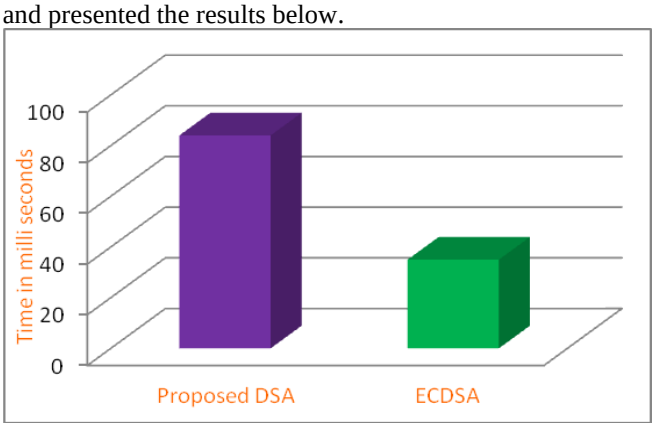

Fig.3. Performance Comparison of Signature Generation over EC P-160

From figure-3, proposed Digital Signature scheme performed poorly because security is inversely proportional to performance of the system.

From Figure-4, proposed scheme signature verification algorithm performed better than the existing verification scheme. This is enviable because to the application oriented point of view message is authorized by the individual only once, but verification may be required many times.

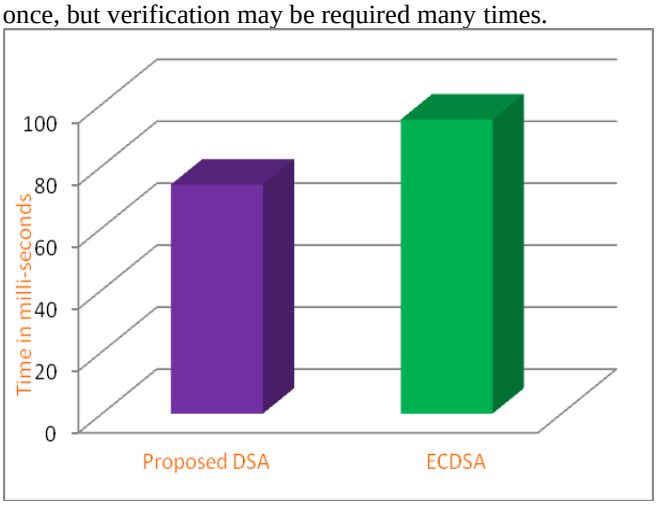

Fig.4. Performance Comparison of Signature Verification over EC P-160.

V. PROOF OF SIGNATURE VERIFICATION

We begin with $W=U_1-U_2$

By substituting U_1 with tG and U_2 with s_1Q

$$W = tG - s_1Q$$

By substituting t with es_2 and Q with dG

$$W = es_{2G} - s_1dG$$

By substituting s_1 with ec and s_2 with (dc + k)

$$W = e(dc + k)_G - ecdG$$
$$= edcG + ekG - ecdG$$
$$= ekG$$
$$= eP$$
$$= R$$

v = X-Co-ordinate(W) and r = X-Co-ordinate(R)

Therefore v = r.

VI. CONCLUSION

Proposed Digital Signature scheme did not use any modular inversion operation. Modular inversion operation is more time consuming operation[12] and our scheme secure even the same random number chosen by the signer in generating more than one signature because it depends on difficulty of ECDLP. Thus, for applications requiring Signature verification more frequently than Signature Generation, proposed scheme may be better choice.

REFERENCES

[1] Araki. Kiyomichi, Takakazu Satoh, and Shinji Miura, "Overview of Elliptic Curve Cryptography," Public Key Cryptography. pp. 2948. Springer-Verlag. 1998.
[2] Rivest, R.L., Shamir, A., and Adelman, L. "A method for obtaining digital signatures and public-key cryptosystem", Commun. ACM, 1978, 21, (2). pp. 120-126.
[3] Elgamal, T, "A public-key cryptosystem and a signature scheme based on discrete logarithms", IEEE Trans. Info. Theo, 1985, IT-31, pp. 469-472.
[4] Koblitz, Neal, "Elliptic Curve Cryptosystem", Mathematics of Computation, vol 48, no, 177, pp 203-209, 1987.
[5] Miller. Victor S., "Use of Elliptic Curves in Cryptography", Lecture Notes in Computer Sci.no. 218, pp. 417-426, Springer-Verlag. 1986.
[6] Vanstone, S. A., "Responses to NISTs Proposal", Communications of the ACM, 35, 50-52, 1992.
[7] T.Yanik, E. Savas and C. K. Koc "Incomplete reduction in modular arithmetic" IEE Proceedings, 2002.
[8] "Digital Signature Standard (DSS)", FIPS Pub.186-2" February 2000.
[9] Certicom Research, "Certicom ECC Challenge", 2009.
[10] H. Lange and W. Ruppert, "Addition laws on elliptic curves in arbitrary characteristics", Journal of Algebra, Vol.107(1),106-116, 1987.
[11] Darrel Hankerson, Alfred Menezes and Scott Vanstone,"Guide to Elliptic Curve Cryptography".
[12] Tao LONG, Xiaoxia LIU, "Two Improvements to Digital Signature Scheme Based on the Elliptic Curve Cryptosystem", Proceedings of the 2009 International Workshop on Information Security and Application, Nov-2009.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)