International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:4, No:2, 2010

Proposed Developments of Elliptic Curve Digital Signature Algorithm

Sattar B. Sadkhan, and Najlae Falah Hameed

***Abstract*—**The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of DSA, where it is a digital signature scheme designed to provide a digital signature based on a secret number known only to the signer and also on the actual message being signed. These digital signatures are considered the digital counterparts to handwritten signatures, and are the basis for validating the authenticity of a connection. The security of these schemes results from the infeasibility to compute the signature without the private key. In this paper we introduce a proposed to development the original ECDSA with more complexity.

***Keywords*—**Elliptic Curve Digital Signature Algorithm, DSA.

I. Introduction

THE DSA was proposed in August 1991 by the U.S. National Institute of Standards and Technology (NIST) [4]. The ECDSA is the EC analog of the DSA [2]. ECDSA was first proposed in 1992 by Vanstone [6]. Hwang et al. [7] presented an authenticated encryption scheme with message linkage. Lee and Chang [9] gave a signature scheme with message linkage recovery which has less traffic and complexity than that of Hwang et al. Recently, Tseng and Jan [10] proposed an authenticated encryption scheme with message linkage and low communication cost. Other research development on signature scheme with message recovery has been published as in articles [3, 11, 13].

In 1985 the Elliptic Curve Discrete Logarithm Problem (ECDLP) was proposed independently as a new cryptographic scheme by Koblitz [5] and Miller [8]. This problem improves the characteristics of the others, increasing the security with the same key sizes [1]. It is considered that the security of elliptic curve cryptography (ECC) is sufficiently proved.

Consider a finite field F_q with characteristic greater than 3. An elliptic curve E over F_q is the set of all solutions $(x,y)\in F_q\times F_q$ to an equation $y^2=x^3+ax+b$, where $a,b\in F_q$ and $4a^3+27b^2\neq 0$, together with a special point O_∞ called the point at infinity, we denote the curve by E/F_q.

It is well known that E/F_q with a binary operation, called addition of points and denoted by $+$, is an abelian group with O_∞ as the identity element. We denote the group by $E(F_p)$. The addition of points is defined as follows: Let be $P=(x_1,y_1)\in E(F_q)$, then $-P=(x_1,-y_1)$. If $Q=(x_2,y_2)\in E(F_p)$, $Q\neq -P$, then $P+Q=(x_3,y_3)$, with $x_3=\lambda^2-x_1-x_2$ and $y_3=\lambda(x_1-x_3)-y_1$, where

$$\lambda=\begin{cases}(y_2-y_1)(x_2-x_1)^{-1}, & P\neq Q,\\ (3x_1^2+a)(2y_1)^{-1}, & P=Q.\end{cases}$$

Defining the curve over a finite field of characteristic 2 or 3 is possible, but it is indifferent for our purposes.

The ECDLP consists of the following: for two points $P,Q\in E(F_q)$, determine the scalar $k\in \mathbb{Z}_n$ such that $kP=Q$ where $n=\#E(F_q)$. It is necessary that P be a generator of the group of points $E(F_q)$, or, at least, that it generates a subgroup with similar number of points.

In this paper we introduce first the original ECDSA, and we will introduce a proposed to development the original ECDSA with more complexity.

II. The Elliptic Curve Digital Signature Algorithm (ECDSA)

The ECDSA is the elliptic curve analog of the DSA. Digital signature schemes are the counterpart to handwritten signatures. A digital signature is a number that depends on the secret key only known by the signer and on the contents of the message being signed. Signatures must be verifiable without access to the signer's private key. Signatures should be existentially unforgeable under chosen message attacks. This asserts that an adversary who is able to obtain Benin's[1] signatures for any messages of his choice cannot forge Benin signature on a single other message.

In this section, we will introduce first the original ECDSA. Suppose Benin wants to send a digitally signed message to Ali. They first choose a finite field F_q, an elliptic curve E, defined over that field and a base point G with order n. Benin's key pair is (d,Q), where d is her private and Q is her public key. To sign a message M Benin does the following:

[1] Here Benin and Ali are two users.

TABLE I
ECDSA SIGNATURE GENERATING

Step 1. Chooses a random integer k with $1 \le k \le n-1$.
Step 2. Computes $kG = (x_1, y_1)$ and $r = x_1 \bmod n$. If $r = 0$ then she returns to step 1.
Step 3. Computes $k^{-1} \bmod n$.
Step 4. Computes $e = h^{-1}(M)$.[2]
Step 5. Computes $s = k^{-1}(e + dr) \bmod n$. If $s = 0$ then she returns to step 1.
Step 6. Benin signature for the message M is (r,s).

To verify Benin's signature (r,s) on the message M, Ali obtains an authentic copy of Benin's parameters and public key. Ali should validate the obtained parameters, Ali then does the following:

TABLE II
ECDSA SIGNATURE VERIFICATION

Step 1. Verifies that r,s are integers in the interval $[1, n-1]$.
Step 2. Computes $e = h^{-1}(M)$.
Step 3. Computes $w = s^{-1} \bmod n$.
Step 4. Computes $u_1 = ew \bmod n$ and $u_2 = rw \bmod n$.
Step 5. Computes $X = u_1 G + u_2 Q$. If $X = O_\infty$ then he will reject the signature.
Otherwise compute $v = x_1 \bmod n$ where $X = (x_1, y_1)$.
Step 6. Accepts the signature if and only if $v = r$.

If the signature (r,s) on the message M was indeed generated by Ali, the $s = k^{-1}(e + dr) \bmod n$. With this information we have

$$\begin{aligned} k &\equiv s^{-1}(e + dr) \bmod n \\ &\equiv (s^{-1}e + s^{-1}rd) \bmod n \\ &\equiv (we + wrd) \bmod n \\ &\equiv (u_1 + u_2 d) \bmod n . \end{aligned}$$

Thus $(u_1 G + u_2 Q) = (u_1 + u_2 d)G = kG$ and so $v = r$ as required.

III. PROPOSED DEVELOPMENTS OF ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

In this proposition the original message m need not to be sent, and it needs not to be a point on EC. Suppose secure elliptic curve E over a finite field F_q is chose, and the order of group of points in $E(F_p)$ should be divisible by a large prime n, so that the discrete logarithm problem on elliptic curve E is difficult to solve. Select a base point $G \in E$ with order n, i.e. $nG = O_\infty$ G is public. Benin's private key is $k_{benin} \in [1, n-1]$, $P_{Benin} = k_{Benin} G$ is her public key.

To sign a message m Benin does the following:

TABLE III
ALGORITHM FOR SIGNATURE PROPOSITION

Step 1*. Chooses a random integer k with $1 \le k \le n-1$.
Step 2*. Computes $R = kG = (x,y)$ and $r = xm \bmod n$. If $r = 0$ then she returns to step 1*.
Step 3*. Computes $s = (k + rk_{Benin}) \bmod n$, if $s = 0$ then she returns to step 1*.
Step 4*. Benin signature for the message m is (r,s).

To verify Benin's signature (r,s) on the message m which is not send, Ali get Benin's parameters and her public key. Ali should validate the obtained parameters, Ali then does the following:

TABLE IV
ALGORITHM FOR RECOVERING MESSAGE OF PROPOSITION

Step 1*. Verifies that r,s are integers in the interval $[1, n-1]$.
Step 2*. Computes $X = sG - rP_{Benin} = (x', y')$ and $m = r(x')^{-1} \bmod n$. If $X = O_\infty$ then he refuses to accept this signature.

If the signature (r,s) on the message m was indeed generated by Ali, the $s = (k + rk_{Benin}) \bmod n$. With this information we have

$$\begin{aligned} X &= (sG - rP_{Benin}) \\ &= (k + rk_{Benin})G - rP_{Benin} \\ &= kG + rk_{Benin}G - rP_{Benin} \\ &= kG + rP_{Benin} - rP_{Benin} \\ &= kG \\ &= (x', y') \end{aligned}$$

and so $m = r(x')^{-1} \bmod n$.

IV. CONCLUSION

In this paper we firstly introduce the original ECDSA, where in this scheme the message M must be send with the signature, this paper proposed a new algorithm to sign any digital message which is need not to be point in our EC and also need not to send, where we need a public key for sender only, where the receiver need not to public any key to read the signature message.

REFERENCES

[1] D. Johnson, A. Menezes, *"The elliptic curve digital signature algorithm (ECDSA)"*, Center of Applied Cryptographic Research, University of Waterloo, Technical Report CORR99-34,1999.

[2] Here h is the secure hash algorithm.

[2] Fibíýková, L., *"Elliptic Curve Cryptography over Prime Fields"*, University of Essen, Germany, (2002).
[3] Jian-zhu Lu, Huo-yan Chen, *"New message recovery signature schemes and its security"*, Mini-Micro Systems 24 (4) (2003) 695–697.
[4] Jurisic, A. and Menezes, A., *"Elliptic Curves and Cryptography"*.
[5] N. Koblitz, *"Elliptic curve cryptosystems"*, Mathematics of Computation 48 (1987) 203–209.
[6] Oswald, E., *"Introduction to Elliptic Curve Cryptography"*, Institute for Applied Information Processing and Communication, Graz University Technology, (2002).
[7] S.J. Hwang, C.C. Chang, W.P. Yang, *"Authenticated encryption schemes with message linkages"*, Information Processing Letters 58 (1996) 189–194.
[8] V. Miller, *"Use of elliptic curves in cryptography, in: Advances in cryptology"*, CRYPTO 85,Lecture Notes in Computer Science, vol. 218, Springer-Verlag, 1986, pp. 417–426.
[9] W.B. Lee, C.C. Chang, *"Authenticated encryption schemes with linkage between message blocks"*, Information Processing Letters 63 (1997) 247–250.
[10] Y.M. Tseng, J.K. Jan, *"An efficient authenticated encryption schemes with message linkages and low communication costs"*, Journal of Information and Engineering 18 (2002) 41–46.
[11] Zhi-chen Li, Yi-xian Yang, *"New message recovery signature scheme"*, Acta Electronic Sinica 28 (1) (2000) 125–126.
[12] Zhi-chen Li, Zhong-xian Li, Yi-xian Yang, *"A new forgery attack on message recovery signatures"*, Journal of China Institute of Communications 21 (5) (2000) 84–87.