JSR Publications

Available Online

J. Sci. Res. **3** (1), 75-79 (2011)

JOURNAL OF
SCIENTIFIC RESEARCH

www.banglajol.info/index.php/JSR

Short Communication

An Approach for Embedding Elliptic Curve in Fractal Based Digital Signature Scheme

D. B. Ojha[1*], Ms. Shree[2], A. Dwivedi[3], and A. Mishra[3]

[1]Department of Mathematics, R.K.G.I.T., U.P. Technical University, U.P, India

[2]Department of Mathematics, S.I.E.T., U.P. Technical University, U.P, India

[3]Department of Master of Computer Applications, R.K.G.E.C., U.P. Technical University, U.P, India

Received 1 April 2010, accepted in final revised form 19 November 2010

Abstract

We established a new approach for cryptographic digital signature scheme based on Mandelbrot and Julia fractal sets. We have embedded the features of ECC (elliptic curve cryptography) to the digital signature scheme based on Mandelbrot and Julia fractal sets. We offered a digital signature that has advantages of both the fractal based digital signature as well as of elliptic curve digital signature.

Keywords: Fractal; ECC; Digital signature.

doi:10.3329/jsr.v3i1.4694 J. Sci. Res. **3** (1), 75-79 (2011)

1. Introduction

The public key cryptosystem introduced by Diffie and Hellman [1] in 1976, numerous public key cryptosystems have been proposed and implemented. Digital signature is an electronic verification mechanism based on the public-key scheme and is considered as a type of the asymmetric cryptography that is focusing on message authenticity. The digital signature scheme is used to provide a guarantee that the original content of a message is unchanged by unauthorized party, which is known as the data integrity. The assurance that the source of data is as claimed, which is known as message authentication, and the assurance that an entity cannot deny commitments which is known as non-repudiation [2]. The output of the signature process is called the digital signature. Then in 1982 fractal has been coined [3]. The Mandelbrot set, named after Benoit Mandelbrot, is a *fractal*. Fractals are objects that display self-similarity at various scales. Magnifying a fractal reveals small-scale details similar to the large-scale characteristics. Although the Mandelbrot set is self-similar at magnified scales, the small scale details are not *identical* to the whole. In

[*] *Corresponding author*: ojhdb@yahoo.co.in

fact, the Mandelbrot set is infinitely complex. The algorithm to generate it is an equation involving complex numbers. Alia and Samsudin [4] studied the aspects of fractal systems in the treatment of public-key cryptography systems, with focus on Mandelbrot fractal set and Julia fractal set (see Fig. 1).

In digital signature based on public-key algorithms, the private key is used to sign a message, while the public key is used to verify the authenticity of the message.

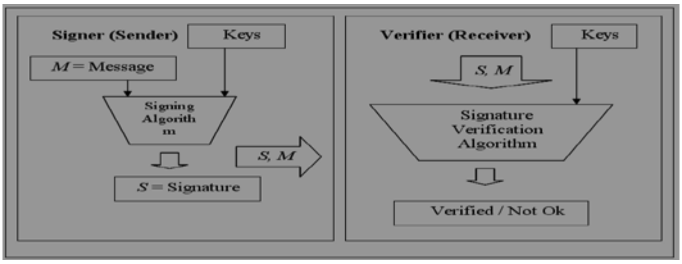

Fig. 1. Digital signature scheme.

The use of elliptic curve in cryptography was introduced by Lenstra's elliptic curve factorization algorithm [5]. Inspired by this sudden unexpected application of elliptic curves in integer factorization, in the mid 1980s, Koblitz [6] and Miller [7] independently introduced the elliptic curve public key cryptography system, a method based on the discrete logarithmic problem over the points on an elliptic curve. The security in elliptic curve schemes is based on the complexity of the elliptic curve discrete logarithm problem. A more detailed discussion on digital signature scheme can be found in refs. [8-11].

In this paper, we introduced a digital signature scheme having properties of fractal based and elliptic curve based digital signature scheme simultaneously to sign and verify the corresponding message.

2. Materials and Methods

The fractal digital signature scheme [6] is to generate the private key and public key by using Mandelbrot function (Eq. 1) and Julia function (Eq. 2).

$$z_n = f(z_{n-1}), z_0 = c; c, z \in C; n \in Z \tag{1}$$

$$z_n = f(z_{n-1}), z_0 = y; y, c, z \in C; n \in Z \tag{2}$$

Fractal digital signature scheme involves a sender and a receiver. The receiver must generate the public key from the chosen private key, and then send the public key to the sender. The sender will then generate his public key by using Mandel function and send it to the receiver.

$$z_n d = z_{n-1} \times c^2 \times d; z, c, d \in C; n \in Z \tag{3}$$

Here $z_n d$ is the generated public key, generated by the receiver by executing equation(3). The receiver's private key is the value (*d*, *n*). Similarly for the sender, with the private value of (*e*, *k*), the sender will produce the corresponding public key, $z_k e$, generated by using Mandel function. The Mandel function is given by

$$z_k e = z_{k-1} \times c^2 \times e; z, c, e, \in C; k \in Z \tag{4}$$

Executing Julia function by the sender will sign the message *m* to produce the signature S. The signature *S* with the message *m*, will then send to the receiver. Similarly, the receiver will execute Julia function to produce *V* which then is used to verify the message *m*.

After exchanging the public keys and executing the Julia function, sender and receiver had completed the secured digital signature scheme. The corresponding signature process is further illustrated by (5) and (6).

$$S = c^{k-x} \times (z_n d)_k e \times m, where\ S, c \in C; n, x, k \in Z, m \in R \tag{5}$$

$$V = c^{n-x} \times (z_k e)_n d \times m, where\ V, c \in C; n, x, k \in Z \tag{6}$$

The variable *x* is used to reduce the final calculation. The value *x* can be set to 0, if desired. Details of ECC scheme can be found in ref. [8-10].

3. Algorithm of Proposed Digital Signature

Choose a sequence of elliptic curve $\wp'(z)^2 = 4\wp(z)^3 - g\wp(z) - h$, where g and h are constants; $\wp$ is the Weierstrass elliptic function and $\wp'(z)$ its derivative. We know that, any digital signature scheme involves a sender and a receiver. As mentioned earlier Mandelbrot and Julia properties were used in the design for this proposed digital signature scheme. In the proposed algorithm, sender and receiver must agree and use the public domain value *c* (a complex number) and a sequence of elliptic curves defined over complex numbers. The sender took an elliptic curve, $y_k^2 = x_k^3 + Ax_k + B$ such that $k \in [1, p-1]$ his private key (k is an integer). The receiver took a elliptic curve $y_n^2 = x_n^3 + ax_n + b$ $n \in [1, r-1]$ his private key (r is an integer). Receiver and sender generated $z_n = x_n + iy_n$ and $z_k = x_k + iy_k$ respectively such that $z_n z_{k-1} = z_k z_{n-1}$, where $z_m = f(z_{m-1}), z_0 = c$, c is a complex number (global information).

Sender chooses (n, d) and receiver chooses (k, e) as their private keys where $e, d \in C$. Now receiver uses Mandelbrot function (Eq. 1) and his private keys to produce the public keys $z_k e$ executing Eq. (3) and sender $z_n d$ respectively.

a. Sender and receiver choose elliptic curves $y_n^2 = x_n^3 + ax_n + b$ and $y_k^2 = x_k^3 + Ax_k + B$, respectively, such that $n \in [1, r-1]$ and $k \in [1, p-1]$, where $a, b, A, B \in F_p, 0 \le x \le p$ and -16(4a^3 + 27b^2) mod $p \neq 0$ both agree on domain value $c \in C$.

b. Sender must generate $z_n = x_n + iy_n$ using *n* and receiver must generate $z_k = x_k + iy_k$ using such that $z_n z_{k-1} = z_k z_{n-1}$, where $z_m = f(z_{m-1}), z_0 = c$, c is a complex number (global information).

c. Sender and Receiver must generate public key from using z_n, and z_k with the help of chosen private values and then send the public key to the each other. The receiver generates his public key by using the equation $z_k e = z_{k-1} \times c^2 \times e; z, c, e \in C$ and $k \in Z$.

d. Sender produces the corresponding public key $z_n d$, generated by using the equation: $z_n d = z_{n-1} \times c^2 \times d; z, c, d \in C$ and $n \in Z$.

e. Now by executing Julia function sender will sign the message m to produce the signature *S*. The signature with the message *m* will then send to the receiver. $S = c^{n-x} \times (z_k e)_n d \times m, S, c \in C, n, x, k \in Z, m \in R$.

f. Similarly Receiver will execute Julia function to produce V which then is used to verify the message m, $V = c^{n-x} \times (z_n d)_k e \times m, V, c \in C, n, x, k \in Z, m \in R$.

g. Signature is valid if $S = V$.

4. Results and Discussion

Let *E* be the sequence of elliptic curves defined over complex numbers and let E_n, E_k be the selected curves. Calculation of the points $z_k e$, $z_n d$ from z_n, z_k by Mandelbrot function depends upon the number of iterations *n, k* as well as the variation constant, *d* and *e*, which makes the Mandel function values jump path chaotically. It is very difficult to mount an attack on the proposed scheme because of the iteration which is unknown to the public. Hence, we can identify that the hard problem for the proposed fractal digital signature is through the chaos property of the fractal function which in this case depends on the private key selection. Our process completely prevents the attack on the private values.

The Elliptic Curve Cryptosystem (ECC) provides the highest strength-per-bit of any cryptosystem known today. Elliptic Curve Cryptosystems (ECCs) are becoming more popular because of the reduced number of key bits required in comparison to other cryptosystems.

Acknowledgement

The authors are thankful to anonymous referees for their valuable suggestions.

References

1. W. Diffie and M. E. Hellman, IEEE Trans.Inform. Theory, IT-**22** (6), 644 (1976). doi:10.1109/TIT.1976.1055638
2. A. J. Menezes, P. C. van Oorschot, and S. A.Vanstone, Handbook of Applied Cryptography (CRC Press, 1996) pp. 4-15. doi:10.1201/9781439821916

3. B. B. Mandelbrot, The Fractal Geometry of Nature (W. H. Freeman and Company, San Francisco, 1982).
4. M. Alia, and A. Samsudin, American Journal of Applied Sciences **4** (11) 850 (2007).
5. A. Lenstra and E. Verheul, Journal to Cryptology **14**, 255 (2001).
6. N. Koblitz, Mathematics of Computation **48**, 203 (1987). doi:10.1090/S0025-5718-1987-0866109-5
7. V. S. Miller, Use of elliptic curve in cryptography, Advances in Cryptology- CRYPTO'85 (Santa. Barbara, Calif., 1985), LNCS 218 (Springer-Verlag, 1986).
8. A. A. Lysyanskaya, PhD thesis, Massachusetts Institute of Technology (2002) pp. 1-3.
9. H. Peitgen, and D. Saupe (eds.), The Science of Fractal Images (Springer-Verlag, New York, 1988).
10. W. B. Schultz, Electronic Records; Electronic. Signatures, Federal Register **62** (54), 13430 (2007).
11. Public Law, Weekly Compilation of Presidential Documents, PUBLIC LAW **106-229** (36), 464 (2000).