Available online at http://scik.org

J. Math. Comput. Sci. 4 (2014), No. 2, 471-478

ISSN: 1927-5307

A KEY AGREEMENT PROTOCOL BASED ON SUPERIOR FRACTAL SETS

SHAFALI AGARWAL[1] AND ASHISH NEGI[2]

[1]Research Scholar, Singhania University, Rajasthan, India

[2]Dept. of Computer Science, G.B. Pant Engg. College, Pauri Garwal, Uttarakhand, India

Abstract. The fractal properties endeavour of inventing new techniques because of its complex structure. Mandelbrot and Julia sets are created by using the same function but in different parameter plane. This strong connection of fractals leads its use in the field of cryptography. In the proposed protocol, superior Mandelbrot set function is used to calculate the public keys with the help of chosen private keys as input parameter whereas superior Julia set function is used to generate a shared private key by using public keys of either side for both parties which is not easy to crack by an intruder.

Keywords: Superior Mandelbrot set, Superior Julia set, Fractal Cryptography, Key Agreement Protocol.

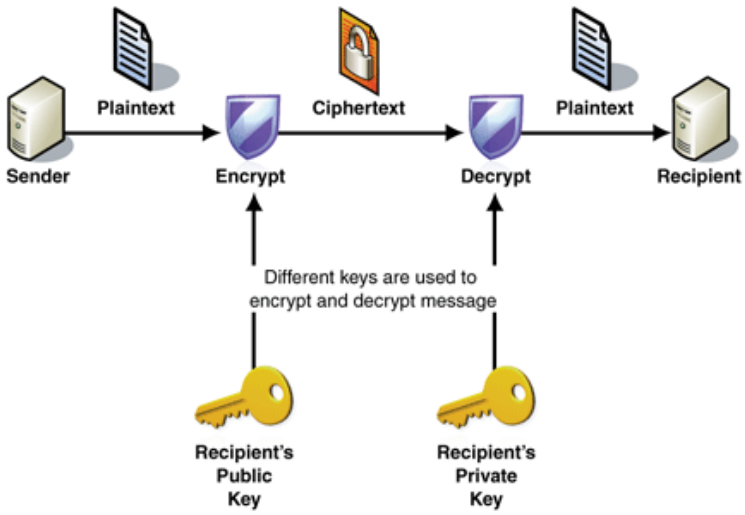
2010 AMS Subject Classification: 37F45.

1. Introduction

An invention is thought as a sequence of various questions and answers. Every researcher may suggest a new path to search out a solution and other might visualize it as an ever expanding island. Cryptography is a unique way to encrypt and decrypt the data transmitted in the network. Encryption is a technique used to convert plain text into cipher text and cipher text is converted into plain text by decryption [12].

*Corresponding author

Received February 20, 2012



It not even ensures that the data does not get read by intruder, but also make sure that the data in transit can't be altered. Cryptography can be achieved with any of two methods: a traditional method, based on the application of number theory and algebra and another based on the application of theory of dynamical system.

Diffie and Hellman were the first to invent to utilize public key concept to exchange the shared key [5]. The concept was to calculate shared key based on the prime numbers existed in available key size. After a long time M.Alia et al. [7] proposed key exchange protocol based on Mandelbrot set and Julia set. A comparative study with Diffie & Hellman protocol is also carried out by the author in the paper [2]. Earlier an author described a cryptographic public key encryption protocol using fractal concept which states that this approach is much superior to public key encryption protocol based on traditional number theory. Recently various fractal structures like bird of pray, water plane fractal, burning ship etc have been studied with respect to fractal orbit [6]. A detailed fractal geometry especially speed of its generation is utilized in encryption process. Before invention of public key algorithm with fractal, an author had reviewed various public key algorithms such as DS, RSA, ECDH etc and its applications like key exchange, data encryption and digital signature [1]. A fundamental explanation about the number theory particularly in the field of cryptography is discussed by Neal Koblitz[10].

Fractals are re-creatable because of their sensitivity to any change in initial condition and it leads to unpredictable behaviour [4]. Mandelbrot set is invented by B.B. Mandelbrot in 1971

[3]. In 2005, Mamta Rani had formulated superior Mandelbrot set and superior Julia set after applying Mann iteration method [8, 9] to the basic Mandelbrot function.

Superior Mandelbrot Set:

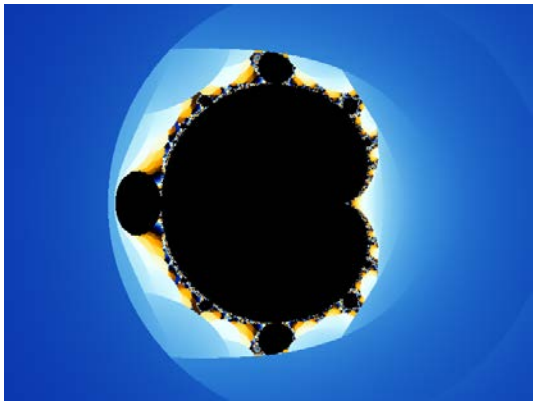
Initially the iteration method is given by W.R. Mann[11]

$$z_{n+1} = s * f(z_n) + (1-s) * z_n \qquad (1.1)$$

where z is a complex number and $0<s<1$ and s is convergent to a non-zero number.

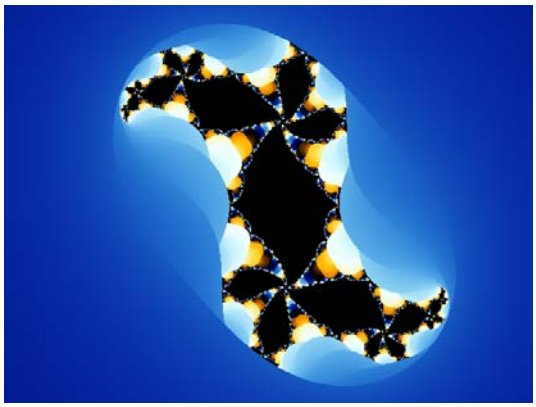
A Superior Mandelbrot set SM for a function of the form $Q_c(z) = z^n + c$, $n = 1, 2,...,$ is defined as the collection of $c \in C$ for which the superior orbit of the point 0 is bounded,

SM=$\{c \in C: \{Q_c^k(0): k=0, 1, \ldots\}$ is bounded in SO$\}$.



Superior Julia set:

The set of complex points SK whose orbits are bounded under superior iteration of a function Q is called the filled superior Julia set. A superior Julia set SJ of Q is the boundary of the filled superior Julia set SK.



In this paper the strong connection between superior Mandelbrot set and superior Julia set is utilized to generate secret shared key between sender and receiver. This phenomenon is known as key agreement between involved parties.

2. Proposed Method and Result Discussion

A fractal is constructed by repeated iteration of a function and generates a complex structure as a resultant. The Mandelbrot and Julia set are constructed using same function i.e. z^2+c. The only difference between two is that the Mandelbrot set is a set of points in complex *c*-plane starting at *z=0* whereas Julia set is an image for a fixed *c* value starting nonzero *z*.

In our method, we used superior Mandelbrot set and superior Julia set to generate public key and private key respectively at both sides. The equation used in proposed method is superior Mandelbrot function "supMS" (see eq. 2.1 & 2.2):

$$f(z_n) = z_n * c * e\,;\ c, z \in Z \text{ and } z_0 = c \tag{2.1}$$

$$z_{n+1} = s * f(z_n) + (1-s) * z_n \tag{2.2}$$

and superior Julia set "supJS" (see eq. 2.3, 2.4 & 2.5):

$$f(z_n) = z_n * c * e\,;\ c, z \in Z \text{ and } z_0 = z_n e \text{ (at receiver side)} \tag{2.3}$$

$$f(z_n) = z_n * c * e\,;\ c, z \in Z \text{ and } z_0 = z_k d \text{ (at sender side)} \tag{2.4}$$

Eq. no. (2.5) is common to both sides:

$$z_{n+1} = s * f(z_n) + (1-s) * z_n \tag{2.5}$$

The method is defined in four steps:

Step 1: At sender side

- Sender assumes *e* and *n* as private keys and *c* is a global value which exists in superior Mandelbrot set.
- A public key $z_n e$ is calculated by using *supMS* function which is the Mann iterated form of Mandelbrot set.
- Send this public key to receiver.

Step 2: At receiver side

- Receiver assumes *k* and *d* as private keys and *c* is a global value which exists in superior Mandelbrot set.
- A public key $z_k d$ is calculated by using *supMS* function which is the Mann iterated form of Mandelbrot set.
- Send this public key to sender.

Step 3: At sender side

- Sender further executes *supJS* function by using *e*, *n* and receiver's public key and obtained a secret key $(z_n e)_k d$.

Step 4: At receiver side

- Now receiver executes *supJS* function by using *k*, *d* and sender's public key and obtained a secret key $(z_k d)_n e$.

In our discussion *n* and *k* represents the number of iterations while *e* and *d* are the variation constants and are unknown to public. In step 1 and step 2, sender and receiver exchanged their public keys and then execute *supJS* to obtain corresponding private shared keys. It is impossible to identify the private values with the help of published public keys. It is also suggested that the value of *e* and *d* must be 128 bit value so that 2^{128} possible values can be used for iteration.

Example:

An example is shown to how the public keys are generated by using private values and similarly how *supJS* is used to create shared secret key on both sides.

Sender assumes *e* as a complex value, *n* number of iterations and a value *c*, known to both sides and initialized to a complex value existed in superior Mandelbrot set. Initially sender calculates its public key by executing *supMS* function and obtained $z_n e$ in step 1.

e = 0.015923 – 0.03179523

n = 4

c = 0.325 + 1.5125

s = 0.6

$z_n e$ = .00726 87838 20012 80547 68432 73672 42014 72775 62822 26562 5 + 0.05340

70804 68766 57175 58719 60672 15500 96169 36723 63281 25

Similarly in step 2, receiver also executes *supMS* function and generates its public key $z_k d$ by using private values k,d and common value c complex value.

k = 3

s = 0.6

d = -0.05124761 + 0.12937622

$z_k d$ = .01362 32781 51994 23957 69007 15585 10488 28125 .02853 95204 94632 28033

55960 19222 14179 6875

Now both parties exchange their public keys. Following this process is the calculation of shared keys by using *supJS* function with public key of either side as initial value of *z* in step *3* and step *4*. As a result secret keys $(z_n e)_k d$ and $(z_k d)_n e$ are obtained. We can show that both keys are indeed the same at both sides.

Sender Side:

z= $z_k d$ = .01362 32781 51994 23957 69007 15585 10488 28125 .02853 95204 94632 28033

55960 19222 14179 6875

e= 0.015923 – 0.03179523

n=4

s=0.6

$(z_k d)_n e$ =.00039 73801 56931 42144 45182 37970 34076 54677 67144 22396 67338 87927

53456 36694 24580 15441 89453 125 .00102 76603 99863 00908 15316 14977 06580

87655 78335 18461 12896 27259 12351 64776 96878 50952 14843 75

Receiver Side:

z= $z_n e$ =.00726 87838 20012 80547 68432 73672 42014 72775 62822 26562 5 + 0.05340

70804 68766 57175 58719 60672 15500 96169 36723 63281 25

s=0.6

k=3

d=-0.05124761 + 0.12937622

$(z_n e)_k d$ =.00039 73801 56931 42144 45182 37970 34076 54677 67144 22396 67338 87927

53456 36694 24580 15441 89453 125 .00102 76603 99863 00908 15316 14977 06580

87655 78335 18461 12896 27259 12351 64776 96878 50952 14843 75

3. Conclusion

This is a very fascinating field to use fractal concept in cryptography. This paper utilized the connection between superior Mandelbrot set and superior Julia set and implemented key agreement protocol in cryptography. By using complex value *e* and *d* and large number of iterations increased the complexity level of protocol. By using fractal with cryptography, gave a larger set of key values as compared to Diffie and Hellman algorithm which is based on the prime values existed for a given key size.

Conflict of Interests

The author declares that there is no conflict of interests.

REFERENCE

[1] A. MS. Public key cryptography: Applications, Algorithms and Mathematical Explanation, India, Tata Elexi-2007

[2] Ahmad, A. M. and A. Samsudin, A new public key cryptosystem based on Mandelbrot and Julia fractal sets, Asian journal of Information technology, 6(2007), 567-575

[3] B. B. Mandelbrot, Fractal geometry of nature, San Francisco: W. H. Freeman, 1983.

[4] Barnsley M., Fracals everywhere, 2nd edition, Academic press professional Inc., San Diego, CA. USA, 1993.

[5] Diffie W. and M.E. Hellman, New directions in cryptography, IEEE transactions on information theory, IT-22(1976), 644-654.

[6] I. Motyl, R. Jasek and P. Varacha, Analysis of the fractal structure for the information encrypting process, International Journal of Computers, 6(2012), 224-231.

[7] M. Alia, A samsudin. New key exchange protocol based on Mandelbrot and Julia fractal set, International journal of computer science and network security, 7(2007), 302-307.

[8] M. Rani, V. Kumar. Superior Mandelbrot Set, J. Korean Soc. Math Edu. Ser.: D 8(2004), 279-291.

[9] M. Rani and V. Kumar, Superior Julia set, J Korea Soc Math Educ Ser D Res Math Educations. 8(2004), 261–277.

[10] Neal Koblitz, A course in number theory and cryptography, 2nd edition, springer, pp 235, 1994.

[11] W. R. Mann, Mean value methods in iterations, Proc. Amer. Math. Soc., 4(1953), 506-510.

[12] W. Stalling. Cryptography and Network Security, PHI, 2004