Journal of Computer Science 7 (4): 526-532, 2011
ISSN 1549-3636

Efficiency Analysis for Public Key Systems Based on Fractal Functions

[1]Nadia M.G. AL-Saidi, [1]Mohamad Rushdan Md. Said and [2]Adil Mahmood Ahmed
[1]Institute for Mathematical Research (INSPEM), University Putra Malaysia,
43400, Serdang, Darul Ehsan, Malaysia
[2]Department of Mathematics, Faculty of Science, Taiz University, Yemen

Abstract: Problem statement: In the last decade, dynamical systems were utilized to develop cryptosystems, which ushered the era of continuous value cryptography that transformed the practical region from finite field to real numbers. **Approach:** Taking the security threats and privacy issues into consideration, fractals functions were incorporated into public-key cryptosystem due to their complicated mathematical structure and deterministic nature that meet the cryptographic requirements. In this study we propose a new public key cryptosystem based on Iterated Function Systems (IFS). **Results:** In the proposed protocol, the attractor of the IFS is used to obtain public key from private one, which is then used with the attractor again to encrypt and decrypt the messages. By exchanging the generated public keys using one of the well known key exchange protocols, both parties can calculate a unique shared key. This is used as a number of iteration to generate the fractal attractor and mask the Hutchinson operator, so that, the known attacks will not work anymore. **Conclusion:** The algorithm is implemented and compared to the classical one, to verify its efficiency and security. We conclude that public key systems based on IFS transformation perform more efficiently than RSA cryptosystems in terms of key size and key space.

Key words: Iterated Function System (IFS), fractal attractor, Hutchinson operator, public key system, fractals functions

INTRODUCTION

The digital information revolution has brought about changes in our society and our lives. Its many advantages have also generated new challenges and new opportunities for innovation. New technology and new applications bring new threats and drives us to invent new protection mechanisms. With this rapid development in information technology, there is a growing demand for cryptographic techniques, which has spurred a great deal of intensive research activities in the study of cryptography (Menezes *et al*., 1997). Since the 1990s, several researchers have observed that there exists an interesting relationship between chaos, fractal and cryptography. Many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems. They are characterized by sensitive dependence on initial conditions and similarity to random behavior, a part from geometrical and statistical complexity, that explain to why this application field qualifies for encryption purposes. Dynamical systems theory is closely related to fractal geometry. One can show that fractals attractors of iterated function systems in particular have a naturally associated dynamical system which is chaotic. Fractals are attractors of dynamical systems; the place where chaotic dynamics occur (Jacquin, 1992).

For details on the relationship between chaos and fractals, refer to (Becker and Dorfler, 1989; Barnsley, 2000).

In recent years, many studies on chaos-based cryptosystems have been published. Much work has been done by incorporating chaotic maps into the design of symmetric and asymmetric encryption scheme. In 2003, (Kocarev *et al*., 2003; Kocarev *et al*., 2005) proposed a public key encryption algorithm based on Chebyshev chaotic maps. Since then many studies on a new key agreement protocol based on chaotic maps were undertaken (Gonzalo, 2005;

Yoon and Yoo, 2008). There were also proposals for incorporating fractal functions into the design of symmetric and asymmetric encryption schemes using the similar mechanism (Ahmad and Samsudin, 2007; Ali and Ahmad, 2008; AL-Saidi and Said, 2009; Kumar, 2006). However though many of the proposed schemes have several advantages such as computational efficiency, ease of generating public-private key pairs, they fail to explain or do not possess a number of

Corresponding Author: Nadia M.G. Al-Saidi, Institute for Mathematical Research, University Putra Malaysia, 43400, Serdang, Selangor, Malaysia Tel : +60162144183/+603 8946 6878 Fax: +603 89423789

features that are fundamentally important to all kinds of cryptosystems. Fractal geometry and in particular, the theory of fractal functions, has evolved beyond its mathematical framework and has become a powerful and useful tool in the applied sciences as well as engineering.

The realm of applications includes structural mechanics, physics and chemistry, signal processing and cryptography (Massopust, 1997).

The reason for this variety of applications lies in the underlying complicated mathematical structure of fractal functions, specifically their recursive construction. They provide better approximates for certain problems than their classical non-recursive counterparts. This study focuses more on the mathematical aspects of fractal functions and briefly exposes the reader to the latest application of fractal functions in cryptography, namely public key cryptosystems.

The outline of the study is organized as follows; the theoretical concepts of iterated function systems are explained in the materials and method part, while a brief explanation on public key systems is provided also. The core of this study is the result which discusses the application of fractal function in public key systems in addition to designing of new public key system based on IFS transformation as well as software implementation with worked example. In the discussion we deal with security and efficiency aspects, followed by the conclusion.

MATERIALS AND METHODS

Iterated function system: an overview of the major concepts and results of Iterated Function System (IFS) and their application is presented. A more detailed review of the topics are as in (Barnsley, 2000; AL-Saidi *et al*., 2009; Kumar, 2006). The theory of fractal sets is a modern domain of research. Iterated function systems have been used to define fractals. Such systems consist of sets of equations, which represent a rotation, a translation and a scaling. These equations can generate complicated fractal images. Therefore, we need some information on dynamical systems.

Given a metric space (X,d), the space of all nonempty compact subset of X is called the Hausdorff space H(X). The Hausdorff distance h is defined on H(X) by:

$$h(A,B)=\max\{\inf\{\varepsilon>0;\ B\subset N_\varepsilon(A)\}\ \inf\{\varepsilon>0;\ A\subset N_\varepsilon(B)\}\} \quad (1)$$

Definition 1: For any two metric spaces (X,d_X) and (Y,d_Y), a transformation $w:X\to Y$ is said to be a contraction if and only if there exists a real number s, $0<s<1$, such that $d_Y(w(x_i),w(x_j))\le s d_X(x_i,x_j)$, for any $x_i,x_j \in X$, where s is the contractivity factor for w.

The following theorem, known as the contraction mapping theorem, states an important property of contractive transformations of a complete metric space within itself.

Theorem 1: Let $w:X\to X$ be a contraction on a complete metric space (X,d). Then, there exists a unique point $x_f \in X$ such that $w(x_f)=x_f$. Furthermore, for any $x\in X$, we have $\lim\limits_{n\to\infty} W^{\circ n}(x)=x_f$, where $w^{\circ n}$ denotes the n-fold composition of w.

A fractal is constructed from a collage of transformed copies of itself. It is inherently self-similar and infinitely scalable. The transformation is performed by a set of affine maps. An affine mapping of the plane is a combination of a rotation, scaling, a sheer and a translation in R^2.

Definition 2: Any affine transformation $w:R^2\to R^2$ of the plane has the form:

$$\begin{pmatrix} u \\ v \end{pmatrix} = W\begin{bmatrix} x \\ y \end{bmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} = A\vec{X}+b \quad (2)$$

where (u,v), (x,y) $\in R^2$, are any point on a plane.

By considering a metric space (X,d) and a finite set of contractive transformation $w_n : X\to X$, $1\le n\le N$, with respective contractivity factors s_n, we proceed to define a transformation W: H(X)→H(X), where H(X) is the collection of nonempty, compact subsets of X, by:

$$A = W(B) = \bigcup_{i=1}^{N} w_i(B) \qquad \textit{for any B H(X)} \quad (3)$$

It is easily shown that W is a contraction, with contractivity factor $s=\max_{1\le n\le N} s_n$. The mapping W is usually referred to as Hutchinson operator. It follows from the contraction mapping theorem that, if (X,d) is complete, W has a unique fixed point $A\in H(X)$, satisfying the remarkable self covering condition:

$$A = W(A) = \bigcup_{i=1}^{N} w_i(A) \quad (4)$$

Definition 3: A hyperbolic IFS $\{X;\ w_1,w_2,\ldots,w_n\}$ consists of a complete metric space (X,d) and a finite set of contractive transformation $w_n:X\to X$ with contractivity factors s_n, for n=1,...,N. The contractivity factor for the IFS is the maximum s among $\{s_1,\ldots,s_N\}$.

The attractor of the IFS is the unique fixed point in H(X) of the transformation W defined by (3).

Public key systems: Following the publication of W. Diffie and Hellman study "New Direction in Cryptography" in (Diffie and Hellman, 1976), new explosion of researches emerged. Their study showed for the first time that secret communication was possible without any transfer of secret key between sender and receiver. Public key systems are designed according to the following principles:

- The keys that are used in encryption and decryption are different
- The encryption key are public
- The decryption keys are keep secret and it is infeasible to compute the secret key by knowing the public one

Numerous public-key algorithms have been proposed. RSA, Rabin and ElGamal are the three widely used public-key systems. RSA system is a public key algorithm, named after its inventors Rivest, Shamir and Adleman. The security of the RSA system is based on the difficulty of factoring integer that are the product of two large prime numbers of approximately equal size. The security of Rabin algorithm is also based on the intractability of factoring integer, while the security of the ElGamal algorithm is based on the difficulty of the discrete logarithm problem (Menezes *et al*., 1997). In a public-key encryption system each entity A has a public key e and a corresponding private key d. In secure systems, the task of computing d given e is computationally infeasible. The public key defines an encryption transformation E_e, while the private key defines the associated decryption transformation D_d. Any entity B wishing to send a message M to A obtains an authentic copy of A's public key e, uses the encryption transformation to obtain the ciphertext $c=E_e(M)$ and transmits c to A. To decrypt c, A applies the decryption transformation to obtain the original message $M=D_d(c)$.

Public-key systems are considered to be slower than private (symmetric) key systems, so that they are used to encrypt small data items and preferable to be used as a key exchange in symmetric systems to protect the real data (Xiang *et al*., 2005). All the three encryption algorithms RSA, Rabin and ElGamal are based on their mechanism on the following system:

$$X_{n+1} = (X_n)^p \pmod N \qquad (5)$$

where, X is an integer, $0 \le X \le N-1$ and M, p and N are properly chosen integers. From the dynamical point of view all three schemes use the following property of (5):

$$(X^p)^q = X^{pq} \pmod N \qquad (6)$$

Given that the RSA algorithm and Rabin public-key encryption scheme use some properties of (6) related to the period of the sequence X_1, X_2, X_3 (mod N), the question arises if another dynamical system can be used in public-key encryption algorithms?

Public key system using IFS transformation: While all the currently used cryptosystems are based on number theory work, it is important to construct public-key algorithm based on dynamical systems by using fractal and chaotic dynamics properties. There have been a number of attempts in this aspect. Due to their complicated mathematical structure, specifically their recursive construction, fractal functions has become a powerful and useful tool in the applied sciences (Massopust, 1997). They provide better approximates than their classical non-recursive counterparts, apart from their advantage in storing only few parameters. This kind of key is very robust to attacks for two reasons. Firstly, the attacker manages to obtain parts of the key (or almost the entire key), but a small digit is missing or the order of the affine mappings is changed, then the fractal image is changed dramatically. In this case the attacker has no way of extrapolation the rest of the key. Secondly, the brute force attack will not work since a fractal key is time consuming to generate especially at high zoon levels. To reduce the computation cost and increase the security of the public-key systems, a new public-key cryptosystem based on fractal is proposed. Most of the previous works in fractal cryptography protocols were designed to be used for symmetric approaches. In this study, the proposed protocol is for an asymmetric approach. This method is based on choosing a known fractal set and upon solving their recursive affine transformation functions, it is used as a key in encryption and decryption algorithms of public key systems. Fractals can be generated by the iteration of one or more affine transformations. In the proposed protocol, the sender and receiver must agree on the chosen IFS function.

Fractal method: To generate fractal attractor, the Hutchinson operator is constructed based on a given affine transformation. Consider an IFS consisting of the maps:

$$w_i(x,y) = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e_i \\ f_i \end{pmatrix}, \quad i = 1,2,...,N \qquad (7)$$

Instead of writing them as above, they can be written in a matrix form (AL-Saidi and Said, 2009):

$$\begin{pmatrix} a_1 & b_1 & c_1 & d_1 & e_1 & f_1 \\ & & \dots\dots\dots & & & \\ & & \dots\dots\dots & & & \\ a_2 & b_2 & c_2 & d_2 & e_2 & f_2 \\ a_N & b_N & c_N & d_N & e_N & f_N \end{pmatrix} \qquad (8)$$

To explain this method, fractal generated using IFS of four affine transformation (w_1,w_2,w_3,w_4) are used, where the generalized case can be easily followed. Fractals generated by affine transformation (9) satisfy the semi-group property:

$$w_i(x,y) = \begin{pmatrix} a_i & 0 \\ 0 & d_i \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} c_i \\ d_i \end{pmatrix}, \ i = 1,2,\dots,N \qquad (9)$$

A dummy coordinate Z which always has the value 1 is added to represent the translation in the affine transformation to represent them as homogenous matrix and the 2-dimensional matrix (9) are structured by (3 by 3) matrix as in (10):

$$w_i(x,y,1) = \begin{pmatrix} a_i & 0 & c_i \\ 0 & b_i & d_i \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \ i = 1,2,\dots,N \qquad (10)$$

Then the 4-affine transformations in (9) are arranged in a (4 by 4) matrix in (11):

$$H = \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix} \qquad (11)$$

We calculate the Hutchinson operator $W=w_4w_3w_2w_1$ and represent it in the form of (10), as:

$$W(x,y,1) = \begin{pmatrix} A & 0 & C \\ 0 & B & D \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \qquad (12)$$

Where:
$A = a_4a_3a_2a_1$, $A \neq 1$.
$B = b_4b_3b_2b_1$, $B \neq 1$,
$C = a_4a_3a_2c_1+a_4a_3c_2+a_4c_3+c_4$
$D = b_4b_3b_2d_1+b_4b_3d_2+b_4d_3+d_4$

This W is used to generate the attractor, without dealing with iteration process. The attractor is then generated by computing W^n for large n.

RESULTS

The proposed algorithm: To conceal the value of fractal attractor during the transmission process, a shared secret key is needed, which is available only to the sender and the receiver. A DH key agreement protocol is used in generating the number of iteration to create the fractal attractor, which in turn is used to generate the public key and encrypt the message. The fractal public key scheme comprised three parts: Key Generation, Encryption and Decryption.

Key generation: Initially the parameters (matrix H, g, p) are regarded as public knowledge (where $g \in Z$ and p is prime number):

- Generate numbers (x,y s), (x',y',r) as receiver and sender private keys, where $x,y,x',y' \in R$ and $r,s \in Z$.
- Calculate and exchange $F_s=g^s$ (mod p), $F_r=g^r$ (mod p) as receiver and sender public key.
- After receiving F_r, the receiver calculates a private shared key $n=(F_s)^r$ (mod p), that is used as the number of iteration in generating fractal attractor W^n:

$$W^n = \begin{pmatrix} A^n & 0 & (T_n(A))C \\ 0 & B^n & (T_n(B))D \\ 0 & 0 & 1 \end{pmatrix}$$

where, $T_n(A)=A^{n-1}+A^{n-2}+\dots+A+1$ and $T_{\underline{n}}(B)= B^{n-1}+B^{n-2}+\dots+B+1$.
By using W^n the receiver and sender public key $(u,v,1)= W^n(x,y,1)$ and $(u',v',1)= W^n(x',y',1)$ are calculated and exchange, where:

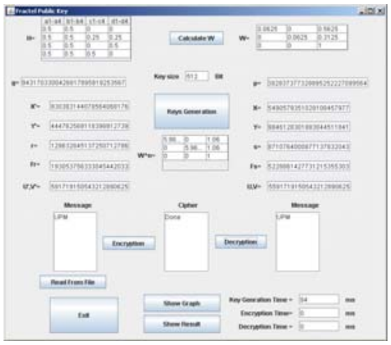
$$u = A^n x + T_n(A)C$$
$$v = B^n y + T_n(B)D$$

And:

$$u' = A^n x' + T_n(A)C$$
$$v' = B^n y' + T_n(B)D$$

Encryption:

- Determine the message to be encrypt and represent it as pairs $M=(m_1,m_2)$
- The sender uses fractal attractor W^n with his private key (x',y'), to find the cipher text Z, such that $Z=(z_1,z_2)=W^n(m_1ux',m_2vy',1)$
- Send the cipher text (Z,,(u',v')) to the receiver



H= a1-a4	b1-b4	c1-c4	d1-d4
0.5	0.5	0	0
0.5	0.5	0.25	0.25
0.5	0.5	0	0.5
0.5	0.5	0.5	0

W=		
0.0625	0	0.5625
0	0.0625	0.3125
0	0	1

Key size 512 Bit

g= [illegible] p= [illegible]

X'= [illegible] X= [illegible]

Y'= [illegible] Y= [illegible]

r= [illegible] s= [illegible]

Fr= [illegible] Fs= [illegible]

U',V'= [illegible] U,V= [illegible]

W^n=		
5.96...	0	1.06
0	5.96...	1.06
0	0	1

Message: LPM

Cipher: Done

Message: LPM

Key Generation Time = 94 ms

Encryption Time= 0 ms

Decryption Time = 0 ms

Fig. 1: Fractal public key user interface

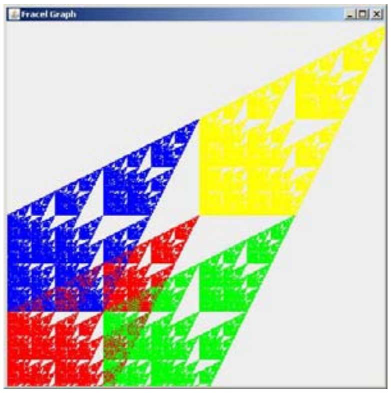


Fig. 2: Fractal attractor for the given IFS

Decryption: Choosing the matrix H as in (11) ensures that W^n is commutation under composition, so due to this semi-group property, if $Z=W^nM$, it follows that $M=W^{-n}Z$.

After receiving (Z,(u',v')), the receiver uses his private key (x,y) and the fractal attractor W^n, the message $M=(m_1,m_2)$ is recovered using:

$$M=(m_1,m_2)=\begin{pmatrix}\dfrac{s_1-T_n(A)C}{(A^nx+T_n(A)C)(u'-T_n(A)C)}\\ \dfrac{s_2-T_n(B)D}{(B^ny+T_n(B)D)(v'-T_n(B)D)}\end{pmatrix}$$

Software implementation: The algorithm and its graphic user interface Fig. 1 are carried out using Java under Net-Beans IDE 6.8. The message transforms to its corresponding ASCII codes, with a possibility to be read either from a file or direct input text. Another classical algorithm (RSA) is coded and compared with the aforementioned fractal algorithm under the same environment. Both algorithms use the time and the security as performance parameters. The efficiency of the algorithms is documented and all the results have been obtained using a computer with these specifications: 3.0GHz Intel (Cor.2 Duo) CPU and 2GB RAM.

Working example: The IFS transformations used in this example are as follows:

$$H=\begin{pmatrix}0.5 & 0.5 & 0 & 0\\ 0.5 & 0.5 & 0 & 0.25\\ 0.5 & 0.5 & 0.5 & 0.5\\ 0.5 & 0.5 & 0.25 & 0\end{pmatrix} \tag{13}$$

Fractal attractor of this affine transformation function is illustrated in Fig. 2 and the Hutchinson operator W is:

$$W=\begin{pmatrix}0.0625 & 0 & 0.5\\ 0 & 0.0625 & 0.3125\\ 0 & 0 & 1\end{pmatrix} \tag{14}$$

As the same keys for encryption is used, the first n-digits remain the same. Hence, the precision of the ciphertext can reach n-digit in decimal system. With each message block, different keys are generated.

DISCUSSION

To ensure fast attractor generation, the domain and the co-domain of fractal functions are defined within the infinite subfield (0,1). In this study, a cryptosystem is formalized based on nonlinear fractal functions over (0,1). Fractal algorithm possesses sufficient security to resist some known attacks, applicable on finite field cryptosystems such as, ciphertext only attack, known plaintext attack, chosen plaintext attack and chosen cipher text attack. The aforementioned attacks are considered as time consuming to be involved in solving non-linear systems numerically over the defined infinite subfield. As an example, a brute force attack strategy is based on explores all elements of the field in finding the secret values might be infeasible and fail to break the system with open key space. Hence, some trial and error methods become impossible and the adversary cannot recover the private key. He will find that the attempts along this line are meaningless as even if he can gain access to some secret parameters, because they are generated from random.

The fractal algorithm is able to resist the known attacks due the open key space and big key size. The “cumulative and truncation errors” accompanying the numerical solution of the non-linear system, pose a difficulty for the algorithm to obtain imprecise decimal numbers. Based on fractal properties, which ensure a sufficient level of randomness, introducing some of the blind signature techniques help to increase the security and randomization of the cryptosystem.

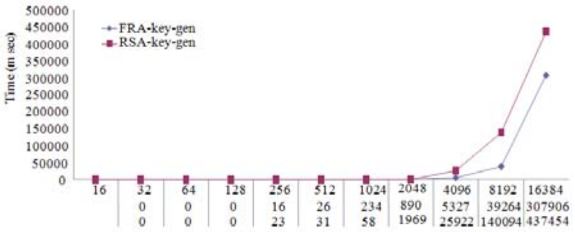


Fig. 3: Fractal and RSA key generation time

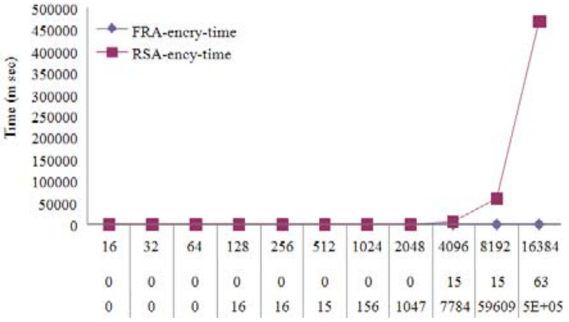


Fig. 4: Fractal and RSA encryption time

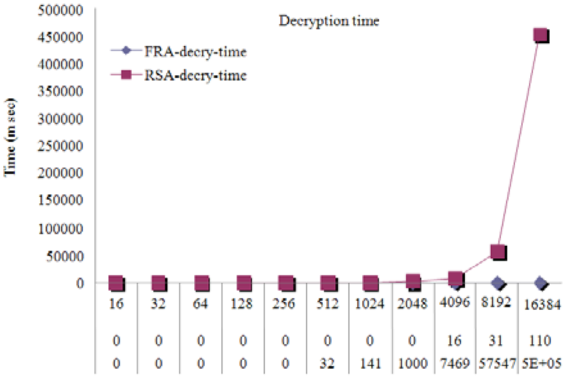


Fig. 5: Fractal and RSA decryption time

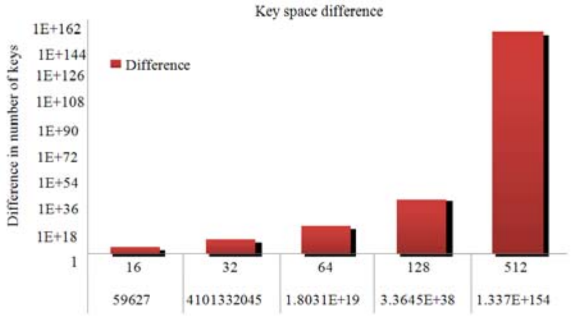


Fig. 6: Fractal and RSA key space difference

(However, multiplying the message with some random reversible values and then removing the randomization after decrypting using their inverse). The inclusion of these random values can helps to ensure a large number of unknown over number of equation and helps to conceal the values of ciphertext through transmission. The adversary found that any attempt along this line is meaningless.

The efficiency of the proposed algorithm is examined in terms of its evaluation parameters. Using the same key size, performance comparison is accomplished between fractal and RSA cryptosystems, as shown in Fig. 3-5. We see that, for fractal system, key generation, encryption and decryption perform better than RSA in terms of time. This is an expected result, as the time needed to calculate the decimal number is less than time needed for integer numbers. Key space comparison Fig. 6 is another security parameter that has to been considered. There are (2^n) fractal key values. The estimated RSA key space value is calculated by (n/log n). Figure 6 shows the key space difference of fractal system among RSA, which is limited by the number of primes in the finite field Z^n, n is the largest value in the key space. This graph is established using (Diff=2^n-2^n/log(2^n)).

CONCLUSION

In this study, a novel fractal protocol is proposed to be used in the public key systems. This is based on the fact that all fractal functions use real number to ensure satisfaction of contraction property. If the cryptosystem parameters are based on real numbers (a continuous infinite interval) then the search space is massive. Hence, many well known attacks fail to solve the nonlinear systems and find the imprecise secret key parameter from the given public one. Even if it is theoretically possible, it is computationally not feasible. After implementing the fractal and the RSA algorithms, we conclude that public key systems based on IFS transformation perform more efficiently than RSA, in terms of key size and key space, apart from its complicated structure to withstand many known attacks.

ACKNOWLEDGMENT

This study is supported by the Institute for Mathematical Research (INSPEM), University Putra Malaysia (Grant no.Vot.5523760) and the authors would like to thank UPM for their cooperation and assistance rendered.

REFERENCES

Ahmad, A.M. and A. Samsudin, 2007. A new public-key cryptosystem based on mandelbrot and julia fractal sets. Asian J. Inform. Technol., 6: 567-575.

Ali, A. and M. Ahmad, 2008. A new approach to public-key cryptosystem based on mandelbrot and Julia fractal sets. PhD Thesis, Universiti Sains, Malaysia. http://eprints.usm.my/8981/

AL-Saidi, N.M.G. and M.R.M. Said, 2009. A new Approach in cryptographic systems using fractal image coding. J. Math. Stat., 5: 183-189. DOI: 10.3844/jmssp.2009.183.189

AL-Saidi, N.M.G., M.R.M. Said and A.M. Ahmed, 2009. IFS On the multi fuzzy fractal space. World Acad. Sci. Eng. Technol., 53: 822-826.

Barnsley, M.F., 2000. Fractals Everywhere. 2nd Edn., Morgan Kaufmann, USA., ISBN-10: 0120790696, pp: 534.

Becker, K.H. and M. Dorfler, 1989. Dynamical Systems and Fractals: Computer Graphics Experiments with Pascal. 1st Edn., Cambridge University Press, USA., ISBN-10: 052136910X, pp: 416.

Diffie, W. and M. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654. DOI: 10.1109/TIT.1976.1055638

Gonzalo, A., 2005. Security problems with a chaos-based deniable authentication scheme. Chaos Solitons Fractal, 26: 7-11. DOI: 10.1016/j.chaos.2004.12.023

Jacquin, A.E., 1992. Image coding based on a fractal theory of iterated contractive image transformations. IEEE Trans. Image Proc., 1: 18-30. DOI: 10.1109/83.128028

Kocarev, L., J. Makraduli and P. Amato, 2005. Public-key encryption based on chebyshev polynomials. Circuits Syst. Signal Process., 24: 497-517. DOI: 10.1007/s00034-005-2403-x

Kocarev, L., M. Sterjev, A. Fekete and G. Vattay, 2003. Public-Key Encryption with Chaos. Chaos, 14: 1078-82. DOI: 10.1063/1.1821671

Kumar, S., 2006. Public key cryptographic system using mandelbrot sets. Proceedings of the IEEE Conference on Military Communications, (MILCOM'06), IEEE Press Piscataway, NJ, USA., pp: 844-848.

Massopust, P.R., 1997. Fractal functions and their applications. Chaos Solitons Fractal, 8: 171-190. DOI: 10.1016/S0960-0779(96)00047-1

Menezes, A.J., P.C.V. Oorschot and S.A Vanstone, 1997. Handbook of Applied Cryptography. 1st Edn., CRC Press, USA., ISBN-10: 0849385237, pp: 780.

Xiang, T., K. Wo Wong and X. Liao, 2005. Security of public-key cryptosystems based on chebyshev polynomials. IEEE Trans. Circuits Syst., 52: 1382-1393. DOI: 10.1109/TCSI.2005.851701

Yoon, E.J. and K.Y. Yoo, 2008. A new key agreement protocol based on chaotic maps. Proceedings of the 2nd KES International Symposium on Agent And Multi- Agent Systems: Technologies and Applications (KES-AMSTA'08), Springer-Verlag Berlin, Heidelberg, pp: 897-906.