An Improved Key Agreement Protocol Based on Fractal Theory

Dr.Nadia M. G. Al-Saidi
Branch of Applied Mathematics, Applied Science Department,University of Technology/ Baghdad
Email: nadiamg08@gmail.com

Received on: 18/3/2013 & Accepted on: 15/8/2013

ABSTRACT

A key agreement protocol is a key establishment technique which enables two or more communicating parities to agree on a key or exchange information over an open communication channel. Due to the complicated mathematical structure and deterministic nature of the fractal functions that meet the cryptographic requirements, and taking the security threats and privacy issues into consideration, a new key agreement protocol based on Iterated Function Systems (IFS) is proposed to provide techniques and tools that may be useful for developing cryptographic protocols. The proposed protocol is a generalization of the Diffie Hellman (DH) protocol. It is designed to overcome some of the drawbacks of several previously proposed key agreement protocols. The experimental results and security analysis shows that the proposed scheme provides an essential security requirement, where their efficiency makes it easier to be applied alone or hybrid with other security methods.

Keywords: Key Agreement, Iterated Function System (IFS); Attractor; Hutchinson Operator W, Diffie Hellman (DH)

بروتوكول الاتفاق على المفتاح المحسن بالاعتماد على الكسيريات

الخلاصة

بروتوكول الاتفاق على مفتاح هو بروتوكول يمكن ان يتفق بموجبهه طرفين او اكثر تتواصل فيما بينها على توليد مفتاح سري مشترك، او ان يتبادلوا المعلومات من خلال قنوات الاتصال المفتوحة. وبسبب الهيكلية والطبيعة الرياضية المعقدة للكسريات والتي تتوافق مع متطلبات انظمة التشفير، وكذلك الاخذ بالاعتبار التهديدات الامنية وتوفير الخصوصية، قمنا باقتراح بروتوكول اتفاق على مفتاح جديد يعتمد على انظمة الدوال المتكررة التي تولد الكيان الكسيري، وذلك لتوفير تقنيات وادوات جديدة قد تكون مفيدة لتطور بروتوكولات التشفير. البروتوكول المقترح هو تعميم لبروتوكول ديفي هلمان DH وقد صمم للتغلب على بعض العوائق الموجودة في العديد من البروتوكولات السابقة. لقد اثبتت النتائج العملية

https://doi.org/10.30684/etj.32.1B.15
2412-0758/University of Technology-Iraq, Baghdad, Iraq

وتحليل الامنية ان النظام المقترح يوفر المتطلبات الاساسية وهو كفوء الى الدرجة التي تجعله سهل الاستخدام كمفتاح متفق علية، او ان يتم تهجينه مع انظمة امنية اخرى .

INTRODUCTION

In network system through insecure channel, there is always needed to establish secure shared key to be used in information transmission. Diffie and Hellman [1] are the first who introduce a key agreement protocol. It is used to drive a shared secret by two or more parties as a function of information contributed by or associated with each of these, but no party can predetermine the result value. A secure key agreement protocol can help communication parities to establish a shared secure secret session key to be used for subsequent communications. Therefore, one of the important goals in information security is how to build a secure key agreement protocol.

Over the past decades, cryptography based on chaos and fractal theory has developed fast. Fractal function was proven as NP hard problem, which means it cannot be solved in a practical amount of time. An IFS provides a convenient framework for the description, classification and communication of fractal. Fractal functions have the potential of creating new ways of securing important information to be transmitted or stored. Some of the proposals for incorporating the fractal functions into the design of symmetric and asymmetric encryption schemes using fractal mechanism are as in [2-7]. Many chaotic based symmetric and asymmetric schemes have been proposed also, as in [8-12].

Recently, fractal and chaos functions have also been used to establish key agreement protocols, some of the proposed protocols in this direction are as [13, 14], also, Xiao et al. [15] in 2007, proposed an original key agreement protocol based on chebychev maps, whereas, in 2008, Yoon and Yoo [16], proposed a new key-agreement protocol based on chaotic maps that could reduce the number of communication rounds. The aforementioned proposals have some security drawbacks. Therefore, in order to enhance the security, and overcomes these drawbacks, a new key agreement protocol based on Iterated Function Systems (IFS) works like DH algorithm that is developed in this paper to provide techniques and tools that may be useful for developing cryptographic protocols.

This paper is organized as follows. In Section 2, a description of some preliminaries of fractal and major concepts of IFS are presented. In Section 3, the fractal method and its application to key agreement protocol are briefly discussed. The software implementation with experimental results is given in Section 4. Section 5 is devoted to discuss the security and performance analysis of the proposed protocol. Finally, the paper is concluded in Section 6.

PRELIMINARIES

Fractal theory is a new discipline that offers a new method to research the self-similarity objects and irregular phenomena. It is an active branch of nonlinear science starting from the 1970s that have proven to be suitable in many fields and particularly interesting in various applications. Some phenomena which cannot be explained with Euclidean geometry could be interpreted with fractal geometry. Fractal theory and its methodology provided people with a new view and new ideas to know the world and made our way of thinking enter into the nonlinear stage. First important advances are

due to M. F. Barnsley [17] who introduced, for the first time, the term "Iterated Function Systems (IFS)" based on the self-similarity of fractal sets. The self-similarity is regarded as a measure of complexity of an image; it is a fundamental characteristic of a fractal used to create them. Regarding to Barnsley, many objects can be closely approximated by self-similarity objects that are generated by using IFS transformations.

Iterated Function System

The term *Iterated Function System* or *IFS* was coined in [18] by Barnsley & Demko to describe a general framework of dynamics. It has been used to define fractals and consist of a number of functions w_1, w_2,…w_n. These functions comprise what is known as IFS. Since the *w*'s only involve a rotation, a translation, and a scaling, this IFS consists of *affine transformations*. These transformations when iterates within the IFS can generate complicated fractal images or *attractor*. This will hold true as long as the mappings in the IFS are all *contractive*. A more detailed theory and definitions of the aforementioned topics are as in [17-22], and as follows.

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

Theorem 1. (*Fundamental Theorem of IFS)*

For any IFS $w=\{w_i\}$,$i=1,\ldots N$ there exists a unique non-empty compact set $A\in R^n$, the invariant *attractor* of the IFS, such that $A=w(A)$.

Theorem 2. (C*ontraction Mapping Theorem)*

Let $w: X\rightarrow X$ 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

$$\lim_{n\rightarrow\infty} w^{\circ n}(x) = x_f \qquad \ldots (1)$$

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

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

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

Definition 3. By considering a metric space (X,d) and a finite set of contractive transformation $w_n:X\rightarrow X$, $1\leq n\leq N$, with respective contractivity factors s_n, we proceed to define a transformation W: $H(X)\rightarrow H(X)$, where $H(X)$ is the collection of nonempty, compact subsets of X, by,

$$A = W(B) = \bigcup_{i=1}^{N} w_i(B) \qquad \ldots (3)$$

for any $B\in H(X)$

It is easily shown that W is a contraction, with contractivity factor $s=\max_{1\leq n\leq N} s_n$. 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.

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

Diffe Hillman Key agreement Protocol

The Diffie-Hellman key agreement protocol was developed by Diffie and Hellman [1] in 1976 and published in the ground-breaking paper "New Directions in Cryptography". Their method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications. It also provides the basis for a variety of authenticated protocols [23].

The simplest, and original, implementation of the protocol uses the multiplicative group of integers modulo *p*,where *p* is prime and *g* is primitive root mod *p*. The algorithm is clarified as in Table (1).

FRACTAL KEY AGREEMENT PROTOCOL

Proposing key agreement algorithms not based on a traditional number theoretical problem is a challenging area of research in information security. A new key agreement protocol based on fractal generating using IFS is proposed in this section to agree on a session key and to ensure the authenticity of the other party. This method is based on choosing a known fractal set, and upon solving their recursive affine transformation functions, it is used as a primitive root to generate the public key. Fractals can be generated by the iteration of one or more affine transformations. In the proposed protocol, the sender and receiver must be agreed on the fractal that used in key establishment.

A. The Proposed Method

Consider an IFS consisting of the maps,

$$w_i(x,y) = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e_i \\ f_i \end{pmatrix}, \qquad \text{i} = 1,2,...,N. \quad \ldots (5)$$

To generate fractal attractor, the Hutchinson operator is constructed based on a given affine transformation. To explain this method, fractal generated using IFS of four affine transformations (w_1, *w2, w3, w4*) are used, where the generalized case can be easily followed. To ensure that the chosen set of transformation satisfy the semi-group property, it should be chosen as in the following general form.

$$w_i(x,y) = \begin{pmatrix} a_i & 0 \\ 0 & b_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} c_i \\ d_i \end{pmatrix}, \; i = 1,2,...,N. \quad \ldots (6)$$

A dummy coordinate *Z* with value 1 is added to represent the translation in the affine transformation, and the 2-dimensional matrix (6) are extended to (3 by 3) matrix as in (7).

$$w_i(x,y,1)=\begin{pmatrix} a_i & 0 & c_i \\ 0 & b_i & d_i \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \qquad i=1,2,...,N. \qquad \ldots (7)$$

The Hutchinson operator $W=w_4w_3w_2w_1$, is calculated and then arrange the coefficient as follows:

$$W(x,y,1)=\begin{pmatrix} A & 0 & C \\ 0 & B & D \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \qquad \text{where} \qquad \ldots (8)$$

$$\begin{aligned} &A= a_4a_3a_2a_1, \quad A\neq 1. \\ &B=b_4b_3b_2b_1, \quad B\neq 1, \\ &C=a_4a_3a_2c_1+a_4a_3c_2+a_4c_3+c_4. \\ &D=b_4b_3b_2d_1+b_4b_3d_2+b_4d_3+d_4. \end{aligned} \qquad \ldots (9)$$

To generate the attractor that should be used in establishing the session key, *W* is iterates to find W^n for large *n*.

Example 1:

The IFS transformations used in this example are as follows:

$$\begin{aligned} w_1(x,y)&=\begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}+\begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ w_2(x,y)&=\begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}+\begin{pmatrix} 0.25 \\ 0.25 \end{pmatrix} \qquad \ldots (10) \\ w_1(x,y)&=\begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}+\begin{pmatrix} 0.25 \\ 0.25 \end{pmatrix} \\ w_1(x,y)&=\begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}+\begin{pmatrix} 0.5 \\ 0 \end{pmatrix} \end{aligned}$$

The Hutchinson operator *W* is calculated using Equations (9) to obtain the following matrix:

$$W=\begin{pmatrix} 0.0625 & 0 & 0.6875 \\ 0 & 0.0625 & 0.1875 \\ 0 & 0 & 1 \end{pmatrix}. \qquad \ldots (11)$$

Fractal attractor of this affine transformation function is illustrated in Figure (1), it is a known fractal example called Sierpinski Triangle.

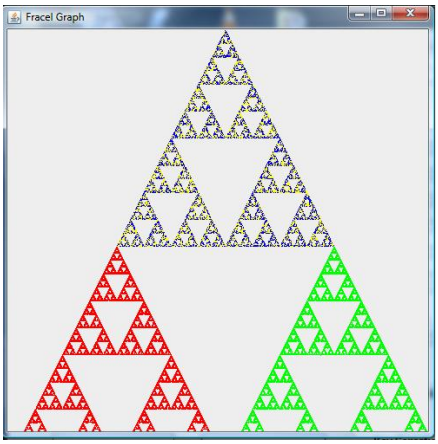

Figure (1) Sierpinski triangle as fractal attractor for the given IFS in (10).

B. The proposed protocol

The protocol involved two parties say Alice and Bob. Both of them must generate their public keys based on their selected private keys. The Hutchinson matrix W must be agreed on and published before performing the agreement protocol, in order to be used as a primitive element in the algorithm. If we suppose that Alice wants to communicate with Bob for establishing session key, then they will perform the following steps.

1- Alice $\rightarrow$Bob :$\{U\}$
   She first chooses three random numbers x, y, and s where $x,y \in R$, $s \in Z$, to compute W^s, and finally computes the public key $U=W^s(x,y,1)$ to be transmitted to Bob.
   Bob$\rightarrow$Alice :$\{U'\}$Bob also chooses three random numbers x', y', and r where $x',y' \in R$, $r \in Z$, to compute W^r, and finally computes the public key $U'=W^r(x',y',1)$ to be transmitted to Alice.
2- Alice after receiving U', uses her private key to calculate the session key $K= W^s*U'*(x, y, 1)$.Bob on the other side after receiving the public key U he uses his private keys x',y',r to calculate the session key $K'= W^r*U*(x',y',1)$.
3- According to the semi group property of this type of fractal matrices in (8), K=K'.
4- Alice and Bob communicate with each other with the shared session key K.

This type of session key is simple; therefore, it is just a basic notion to illustrate the ideas behind fractal based key agreement protocol. There are still many security problems, such as; it is vulnerable to man in the middle attacks, cannot provide user anonymity. Hence it cannot be used directly in practice, a more secure key agreement protocol is performed by sharing a reliable third party (Trent) that used to shares a different secret key with each participant, which is needed to satisfy a secure communication, and to support mutual authentication.

EXPREMENTAL RESULTS AND SOFTWARE IMPLEMENTATION.

The DH algorithm and its generalization using IFS, with its graphic user interface Figure (2, 3), are carried out using Java under Net-Beans IDE 6.8. All the results have been obtained using a computer with the specifications: 3.0GHz Intel (Cor.2 Duo) CPU, and 2GB RAM.

Sierpinski Triangle in example 1 is used to carry out the fractal key agreement protocols. The execution results from the program are as shown in Figure (4). Using different key, the execution of both programs (Fractal key agreement and DH) are performed and compared as illustrated in Table (2).

The efficiency of the proposed algorithm is examined using the same key size and running under the same environments for the fractal key agreement protocol against the DH key agreement protocol, to conclude that the fractal algorithm performs better than DH in terms of execution time. This is an expected result, as the time needed to calculate the decimal number is less than that for integers. Another comparison factor is the key space value that it considers to be open for fractal algorithm comparing to that uses the specific number of primes in the finite field Z^n for some large n, as it is shown in the Figure (5). The key space values is calculated using the equation ($DIFF=2^N-2^N/\ LOG\ (2^N)$).

SECURITY ANALYSIS

In key agreement protocols, the participants do not verify the identity of each other for this reason most of these protocols are vulnerable to many attacks. The security analysis for the proposed protocol is discussed in details to show that the fractal key agreement protocol can withstand several known attacks; some of them are as follows. At the first, let us assume that the attacker has a total control over the communication channel between the two parties.

1- Brute force attack

The domain and the co-domain of the fractal functions are defined within the infinite subfield (0, 1). So, due to open key space and big key size the fractal key agreement protocol is proven to be able to withstand some known attacks among the traditional protocols that based on finite field and deals with discrete log and factorization problem.

2- Replay Attack

Through the reusing of the information obtained in the protocol, an adversary could impersonate the legal user. Even if he obtained U or U' it is not easy for him to recover r or s, because it is the results of iterations and it is a time consuming to go through all values of n for large n.

3- Mutual authentication

The proposed protocol achieves mutual authentication between two parties. In step 2 of the algorithm, Alice calculates K using her private keys x,y,s and Bob also calculates K' using his private keys x',y',r; they agree on the session key if $K=K'$, that means, the mutual authentication is done.

4- Known session key attack

In the proposed protocol, the session key is $K= W^s*U'*(x,y,1)$, or $K'= W^r*U*(x',y',1)$, where $x,y,x',y',r,$ and s are random numbers. Although, the attacker can know previous

session keys, such as; *U* or *U'*, which represent the public key that is computed using the private key (*s* or *r*) as an iteration, and the variation constant (*x*,*y*) or (*x'*,*y'*), he still cannot compute the session key, because the inclusion of these random values can help to ensure a large number of unknown over the number of equations. That is mean, solving the nonlinear system numerically resulted in accompanying of cumulative and truncation errors, and is considered as time consuming over the definite infinite subfield. Hence, it is impossible to find the private key from the given public key.

CONCLUSIONS

An improved key agreement protocol based on fractal functions is proposed in this paper. It is a generalization to the DH protocol, and uses the inherent advantage of fractal attractor in terms of smaller key size. Comparison study is accomplished to prove that the formal is performing better in terms of the execution time and key space. The proposed protocol possesses sufficient security to withstand some known attack that may be applicable to the traditional protocols. Hence, any attempt to find the imprecise secret key parameter from the given public one is redundant.

REFERENCES

[1]. Diffie, W. M. Hellman. "New Directions in Cryptography", IEEE Transaction on Information Theory, vol. 22, no 6, pp.644-654, 1976.

[2]. Kumar, S. Public key cryptography system using Mandelbrot sets, Proceedings of the IEEE Conference, MILCOM 2006, IEEE Press, Piscataway, NJ, USA, 2006, pp.1–5.

[3]. Mohammed and A. Samsudin, A. Generalized scheme for fractal based digital signature, Int. J. Comput. Sci. Netw. Secur. 7(7) (2007), pp. 99–104.

[4]. Mohammed and A. Samsudin, A. A new approach to public-key cryptosystem based on Mandelbrot and Julia, Ph.D. thesis, Universiti Sains, Malaysia, 2008.

[5]. Al-Saidi, N. Md. R. Muhammad Said, Improved Digital Signature Protocol Using Iterated Function Systems, International Journal of Computer Mathematics, 88(17): 3613-3625, 2011.

[6]. Al-Saidi, N. Md. R. Muhammad Said A. M. Ahmed New Direction in Public Key Systems using Iterated Function System. Journal of Computer Science 7 (4): 526-532, 2011

[7]. Al-Saidi, N. Md. R. Muhammad Said, A new approach in cryptographic systems using fractal image coding. Journal of Mathematics and Statistics 5 (3): 183-189, 2009.

[8]. Baptista, M. Cryptography with chaos. Physics Letter A, 240, pp.50-54. 1998.

[9]. Kocarev, L. M. Sterjev, A. Fekete , G.Vattay. "Public-Key Encryption with Chaos", Chaos, Dec; vol. 14, no. 4, pp.1078-82, 2003.

[10]. .Bose, R. "Novel public key encryption technique based on multiple chaotic systems". Phys Rev Lett, vol. 95, 2005.

[11].Wang, X.Y., Chen, F., Wang, T.: A new compound mode of confusion and diffusion for block encryption of image based on chaos. Commun. Nonlinear Sci. Numer. Simul. 15(9), 2479–2485 (2010)

[12].Xiang, T.,Wong, K., Liao, X.F.: An improved chaotic cryptosystem with external key. Commun. Nonlinear Sci. Numer.Simul. 13(9), 1879–1887 (2008)

[13]. Yoon, E. I. Jeon. "An efficient and secure Diffie–Hellman key agreement protocol based on Chebyshev chaotic map", Commun Nonlinear Sci Numer Simulate, vol.16, no.6 , pp. 2383–2389, 2011.
[14]. Alia, M. and A. Samsudin,. "New Key Exchange Protocol Based on Mandelbrot and Julia Fractal Sets'. IJCSNS International Journal of Computer Science and Network Security, vol. 7, no.2, 2007.
[15]. Xiao, D. X. Liao, and S. Deng. "A novel key agreement protocol based on chaotic maps'. Inform. Sci. vol. 177, pp.1136–1142, 2007.
[16]. Yoon, E.J. K. Y.Yoo. "A New Key Agreement Protocol Based on Chaotic Maps". In Proceeding of the second KES international symposium on agent and multi-agent systems: Technologies and Applications (KES-AMSTA '08), Mar., 897-906. 2008.
[17]. Barnsley, M. Fractals Everywhere. Academic Press Professional, Inc., San Diego, CA, USA, second edition, 1993.
[18]. Barnsley and S. Demko, M.F."Iterated function systems and the global construction of fractals', Proc. Roy. Soc. London A399, pp. 243-275, 1985.
[19]. Hutchinson. J. "Fractals and self-similarity". Indiana University Mathematics Journal, vol. 30, no. 5 , pp. 713–747, 1981.
[20]. Dugelay, J.L. E. Polidori and S. Roche. Iterated Function Systems for still Image Processing. IWISP-96, Manchester, UK, November. Indian Institute of Technology Bombay. Mumbai. 1996.
[21]. Massopust, P. R. "Fractal Functions and their Applications", Chaos, Solitons and Fractal, vol. 8,no. 2, pp. 171-190. 1997.
[22]. Nikiel, S. Iterated Function Systems for Real-Time Image Synthesis, Springer-Verlag London Limited., 2007.
[23]. Stallings, W. Cryptography and Network Security: Principles and Practice, Prentice Hall. 5th Edition, 2010.

Table (1) Diffie Hellman protocol.

Alice				**Bob**		
Secret	**Public**	**Calculates**	**Sends**	**Calculates**	**Public**	**Secret**
a	p, g		p,g⟶			b
a	p, g, A	$g^a \bmod p = A$	A⟶		p, g	b
a	p, g, A		⟵ B	$g^b \bmod p = B$	p, g, A, B	b
a, s	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b, **s**

Table (2) Performance Comparison.

	Fractal key agreement		DH protocol	
No. of Bits	Generating time	Key agreement time	Generating time	Key agreement time
128	57	0	13	10
256	90	0	50	12
512	103	0	73	29
1024	152	4	139	164
2048	350	9	267	1124
4096	891	14	704	8235
8192	2377	22	1875	59722

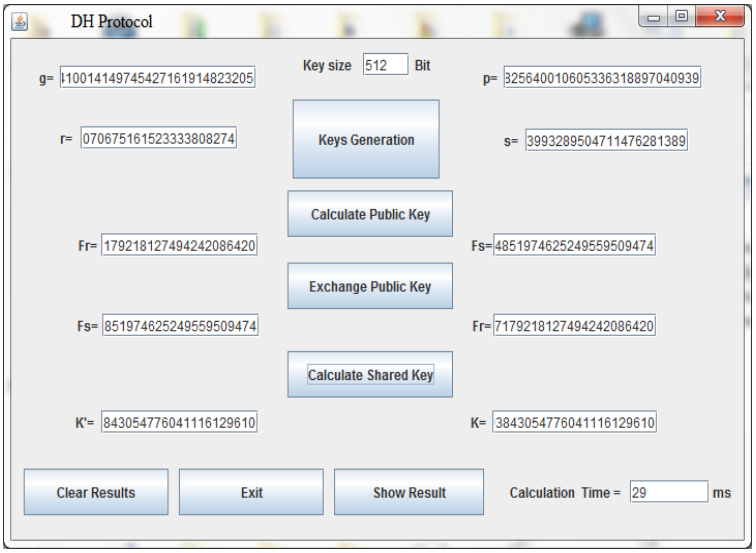

Figure (2) Diffie Hellman user interface.

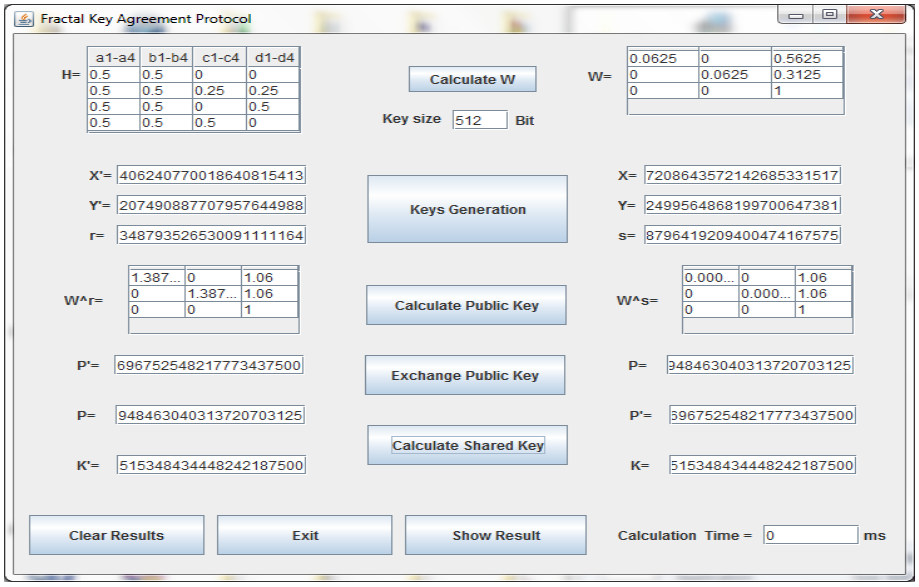

Figure (3) Fractal key agreement user interface.

Var.	Variable Value	No. D
X	0.133875057006593214051428095343 29...	130
y	0.569575872969166249252341370555 45...	130
s	58041835790124665218907674339944 2...	128
X'	0.935929257766858688308079210043 44...	130
Y'	0.036636449389188494587350169584 40...	130
r	48506811426721510935874659741694 4...	128
Pu	0.596252042771255593768524954652 33...	146
Pv	0.331258691038100725803363835775 30...	146
Pu'	0.596250000217913011500346168947 42...	162
Pv'	0.331250000008530088092477176009 52...	162
K1	0.355515280632292226038000520227 81...	306
K2	0.109729441409196531238317949420 35...	306
K1'	0.355515280632292226038000520227 81...	306
K2'	0.109729441409196531238317949420 35...	306

Figure (4) Fractal key agreement results.

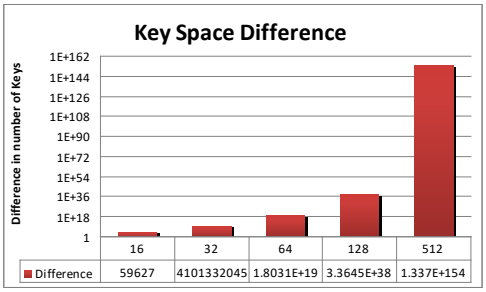

Figure (5) Fractal and RSA key space difference.