World Applied Sciences Journal 15 (3): 364-371, 2011
ISSN 1818-4952

A New Idea in Zero Knowledge Protocols Based on Iterated Function Systems

Nadia M.G. Al-Saidi and Mohamad Rushdan Md Said

Institute for Mathematical Research (INSPEM),
University Putra Malaysia (UPM), 43400, Serdang, Darul Ehsan, Malaysia

Abstract: A secure method of identification is crucial to avoid computer deception dynamics. This could be attained by using zero-knowledge protocols. Zero-knowledge protocols are cryptographic protocols that have been proven to provide secure entity authentication without revealing any knowledge to any entity or to any eavesdropper and used to build effective communication tools and ensure their privacy. Many schemes have been proposed since 1984. Among them are those that rely on factoring and discrete log which are practical schemes based on NP- hard problems. Our aim is to provide techniques and tools which may be useful towards developing those systems. Fractal code was proven as a NP-hard problem, which means it cannot be solved in a practical amount of time. In this paper a new zero-knowledge scheme is proposed based on iterated function systems and the fractal features are used to improve this system. The proposed scheme is a generalization of the Guillou-Quisquater identification scheme. The two schemes are implemented and compared to prove their efficiency and security. From the implementation results, we conclude that zero knowledge systems based on IFS transformation perform more efficiently than GQ system in terms of key size and key space.

Key words: Zero-knowledge · Fractal · Iterated function systems (IFS) · Guillou-Quisquater protocol · Attractor

INTRODUCTION

Following the publication of Diffie and Hellmen [1], new explosion of researches emerged. Their paper showed for the first time that secret communication was possible without any transfer of secret key between sender and receiver. Another proposal is the public key cryptosystem that is based on algebraic coding theory in 1978 by McEliece [2].

The Zero-Knowledge (ZK) Protocol is a method used for authentication. The first party must prove it knows the right password without giving any information about that password to the authenticating second party. This is a method to avoid sending a password over a network that could be detected by a third party. It is proposed at first as a method for exchanging public keys, for creating digital signatures or for protection of digital cash on smart cards. Itis considered as more time-consuming than other authentication methods, but also harder to decipher [3]. With the use of smart cards, user identification and certificate authority are contained and accessed by use of a user personal identification number (PIN).

Where Certificate Authority (CA) can be used for the purpose of securing the exchange of public keys. CAs are servers that could be used for verification; i.e. to certify the issued certificates which include the public keys [4]. Zero knowledge proof (ZKP) was first introduced by Goldwasser, Micali and Rackoff [5] in 1985. The wide applicability of zero-knowledge was demonstrated by Goldreich, Micali and Wigderson in [6]. Fiat and Shamir [7] presented a simple identification and signature scheme that enables any user to prove his identity and the authenticity of his messages. The difficulty of this task is based on RSA problem.

Micali and Shamir [8] presented an improvement to their previous scheme that reduces the verifier's complexity to less than 2 modular multiplications and leaves the prover's complexity unchanged. Although it is computationally fast, it is still based on RSA problem. Fiege et al [9] introduced the notion of interactive proofs of assertions to interactive proofs of knowledge.

Ong-Schnorr identification and signatures [6] are variants of the Fiat-Shamir scheme with short and fast communication and signatures. This scheme uses secret

Corresponding Author: Nadia M.G. Al-Saidi, Department of Applied Sciences, Applied Mathematics University of Technology, Baghdad Iraq. Tel : +9647901305365/+9647712876443.

keys that are square roots modulo N of the public keys. Its security is based on the intractability of certain discrete logarithm problems. It is also proven to be secure against passive and concurrent attacks. Guillou and Quisquater (GQ) identification scheme [10] is an extension to Fiat-Shamir scheme, which reduces the number of exchanged messages and memory requirements for secret keys.

The GQ protocol is an extension of the RSA protocol which reduces the number of rounds needed to 1 and its security is based on the intractability of RSA problem. Goldwasser and Kalai [11] showed that the signature based on Fiat-Shamir (and also Fiege-Fiat-Shamir) is forgeable. Courtois [12] proposed a new Zero-knowledge scheme based on an NP-complete problem known as MinRank. Wolf [13] showed how zero knows proofs can be used to solve authentication problems. All the previous studies are applicable on finite field, so using new systems that work on an infinite field is a new challenge in modern cryptosystems. Alia, M. and A. Samsudin in [14], proposed a new zero-knowledge proof of identity protocol based on Mandelbrot and Julia Fractal sets. They discovered that the security of the proposed fractal zero-knowledge proof of identity is based on the NP-hard problem and the randomness of the output generated. Shuichi Aono, Yoshifumi Nishio, in [15] proposed an authentication protocol using three times the authentication interaction. This authentication protocol is based on iterations of the logistic map in public-key cryptography.

The rest of this paper is organized as follows. Section 2 focuses on the material and methods used in this study; some mathematical preliminaries about the iterated function system are provided. The concepts of zero knowledge protocol/proof, in addition to some existing schemes are analyzed. Section 3 presents the new zero knowledge proof based on IFS and then evaluates the scheme with comparable existing ZKP schemes qualitatively. The algorithms for both methods with their implementation are discussed briefly. The performance and security aspects are analyzed in Section 4 followed by the conclusion in Section 5.

MATERIALS AND METHODS

Iterated Function Systems: The term "iterated function system" (abbreviated: IFS) was coined in [16] by Barnsley & Demko to describe a general framework of dynamics. However, most of the results on the IFS model were shown in [17]. This section presents an overview of the major concepts and results of Iterated Function System (IFS) and their application. A more detailed review of the topics in this section are in [18-20]. The theory of fractal sets is a modern domain of research. Iterated function systems (IFS) 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 [21].

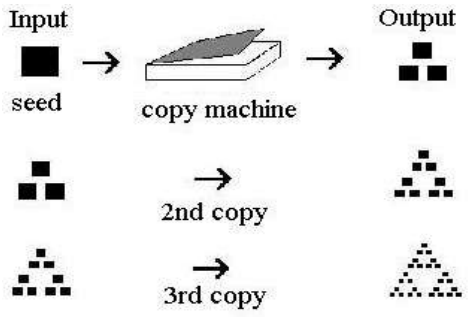


Fig. 1: A copy machine that makes three reduced copies of the input image

The metaphor of a Multiple Reduction Copying Machine Figure (1) is an elegant way to introduce Iterated Function Systems. The MRCM is to be understood as a regular copying machine with the exception that the lens arrangements are such that they reduce the size of the original picture and they overlap copies of the original into the generated copy. Further, the MRCM operates with a feedback loop in which the output of the previous copy is used as the input of the next stage. It doesn't matter with what picture the user begins with. What will determine the attractor, or the output of an iterated function system, will be the rules that are used in the copying, which acts as the iteration [22].

Definition 1: 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 2: 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, $0 \le s \le 1$, such that $d_Y(w(x_i),w(x_j)) < s d_X(x_i,x_j)$, for any $x_i,x_j \in X$, where s is the contractivity factor for w.

An IFS describes a unique set: its attractor. The attractor is invariant under the Hutchinson operator of the IFS and is very often fractal. The following theorem,

fundamental to the study of iterated function systems, asserts that, for any IFS, there always exists such a set. It first appeared in Hutchinson [17].

Theorem 1: (*Fundamental Theorem of Iterated Function Systems*) 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 $A=w(A)$.

Another important property (Theorem 2) of contractive transformations of a complete metric space within itself, is known as the *contraction mapping theorem*,

Theorem 2: Let $w:X\to Y$ 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 $\lim_{n\to\infty} W^{\circ n}(x) = x_f$, where $w^{\circ n}$ denotes the n-fold composition of w.

Definition 3: 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 $w_n : X\to X$, $1=n=N$, with respective contractivity factors s_n, we proceed to define a transformation W: $H(X)\to H(X)$, where $H(X)$ is the collection of nonempty, compact subsets of X, by, $A = W(A) = \bigcup_{i=1}^{N} w_i(B)$ for any $B\in H(X)$ (3)

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

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

Zero-Knowledge Protocol: A lot of theories have been written about zero-knowledge protocols. However not much practical information is available even though zero-knowledge techniques have been used in many applications. Proofs are often seen (by scientists) as a static mathematical object. A "proof" or equivalently a "proof system" is a randomized protocol by which one party (called the prover) tries to convince another party (called the verifier) that the given statement is true. The following names appear in zero-knowledge protocols [23]:

Peggy the Prover: Peggy has some information that she wants to prove to Victor, but without telling the secret itself to Victor.

Victor the Verifier: Victor asks Peggy a series of questions, to find out if Peggy really knows the secret or not. Victor does not learn anything about the secret itself, even if he cheats or does not adhere to the protocol.

Eave the Eavesdropper: Eave is listening to the conversation between Peggy and Victor. A good zero-knowledge protocol also ensures that no third-party comes to know about the secret.

An interactive proof system for a set S is a two party game between a prover and a verifier and it satisfies two properties [24]:

Completeness: Peggy has very high probability of convincing Victor if she knows O$\in$S,

Soundness: Peggy has very low probability to fool Victor if she does not know O. Zero-knowledge protocols having some special features; the verifier cannot learn anything from the protocol, the prover cannot cheat the verifier, the verifier cannot cheat the prover and the verifier cannot pretend to be the prover to any third party .

Example

Ali Baba's Cave (Magical Cave): Consider the non-computer example that illustrates a zero-knowledge proof, the Ali Baba's cave Figure (2), with a secret door that can be opened by a password. Peggy knows the password of the door and wants to convince Victor that she knows it, but doesn't want Victor to know the password itself. They work as follows [1]:

- Peggy goes into a random branch of the cave, which Victor doesn't know as he is standing outside the cave.
- Victor comes into the cave and calls out a random branch of the cave (left or right), where Peggy should come out
- If Peggy knows the secret password, she can come out the right way every time, opening and passing through the secret door with the password if

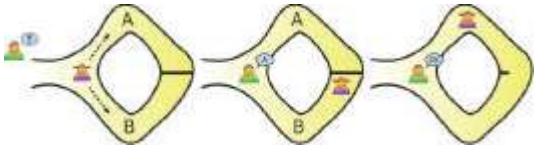


Fig. 2: A magical cave.

necessary. If Peggy doesn't know the password, she has a 50% chance of initially going into the wrong branch and as she is not able to pass the secret door, Victor can call her bluff.

Feige-Fiat Proof of Identity: Feige-Fiat-Shamir was the first practical identity-based protocol. It minimized computation by increasing the number of iterations and accreditations per iteration. However it was less than ideal for some applications, like smart cards. Exchanges with the outside world are time-consuming and the storage required for each accreditation could strain the limited resources of the card.

Before issuing any private keys, the arbitrator chooses a random modulus, *n*, which is the product of two large primes. In real life, *n* should be at least 512 bits long and probably closer to 1024 bits. This *n* can be shared among a group of prover's. (Choosing a Blum integer makes computation easier, but it is not required for security.)

To generate Peggy's public and private keys, a trusted arbitrator chooses a number, *v,* where *v* is a quadratic residue mod *n.* In other words, choose *v* such that $x^2 \equiv v \pmod{n}$ has a solution and $v^{-1} \bmod n$ exists. This *v* is Peggy's public key. Then calculate the smallest *s* for which $s \equiv \text{sqrt}(v^{-1}) \pmod{n}$. This is Peggy's private key [12].

The Identification Protocol Can Now Proceed:

- Peggy picks a random *r,* where *r* is less than *n.* She then computes $x = r^2 \bmod n$ and sends *x* to Victor.
- Victor sends Peggy a random bit, *b.*
- If $b = 0$, then Peggy sends Victor *r.* If $b = 1$, then Peggy sends Victor $y = r * s \bmod n$.
- If $b = 0$, Victor verifies that $x = r^2 \bmod n$, proving that Peggy knows sqrt (*x*). If $b = 1$, Victor verifies that $x = y^2 * v \bmod n$, proving that Peggy knows sqrt (v^{-1}).

This is a single round-called an accreditation-of the protocol. Peggy and Victor repeat these protocol *t* times, until Victor is convinced that Peggy knows *s*.

Guillou-Quisquater Proof of Identity.: Louis Guillou and Jean-Jacques Quisquater [25] developed a zero-knowledge identification algorithm more suited to applications like these. The exchanges between Peggy and Victor and the parallel accreditations in each exchange are both kept to an absolute minimum: There is only one exchange of one accreditation for each proof. For the same level of security, the computation required by Guillou-Quisquater is greater than by Feige-Fiat-Shamir by a factor of three. As with Feige-Fiat-Shamir, this identification algorithm can be converted to a digital signature algorithm.

Peggy is a smart card who wants to prove her identity to Victor. Peggy's identity consists of a set of credentials: a data string consisting of the card's name, validity period, a bank account number and whatever else the application warrants. This bit string is called *J.* (Actually, the credentials can be a longer string and hashed to a *J* value. This complexity does not modify the protocol in any way.) This is analogous to the public key. Other public information, shared by all "Peggys" who could use this application, is an exponent *v* and a modulus *n,* where *n* is the product of two secret primes. The private key is *B,* calculated such that $JB^v \equiv 1 \pmod{n}$.

Peggy sends Victor her credentials, *J.* Now, she wants to prove to Victor that those credentials are hers. To do this, she has to convince Victor that she knows *B.* Here's the protocol [25]:

- Peggy picks a random integer *r,* such that *r* is between 1 and *n* - 1. She computes $T = r^v \bmod n$ and sends it to Victor.
- Victor picks a random integer, *d,* such that *d* is between zero and *v* - 1. He sends *d* to Peggy.
- Peggy computes $D = rB^d \bmod n$ and sends it to Victor.
- Victor computes $T' = D^v J^d \bmod n$. If $T \equiv T' \pmod{n}$, then the authentication succeeds.

To Prove that,
$T' = D^v J^d = (rB^d)^v J^d = r^v B^{dv} J^d = r^v (JB^v)^d = rv \equiv T \pmod{n}$, since *B* was constructed to satisfy $JB^v \equiv 1 \pmod{n}$.

The Proposed Fractal Method for Zero-knowledge Proof: In this section, proof of knowledge scheme based on IFS transformations is detailed as follows.

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

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

Instead of writing them as above, they can be written in a matrix form,

$$\begin{pmatrix} a_1 & b_1 & c_1 & d_1 & e_1 & f_1 \\ & & ..... & & & \\ & & ..... & & & \\ a_2 & b_2 & c_2 & d_2 & e_2 & f_2 \\ a_N & b_N & c_N & d_N & e_N & f_N \end{pmatrix} \tag{6}$$

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 in (7) satisfy the semi-group property.

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

A dummy coordinate Z with value 1 is added to represent the translation in the affine transformation and the 2-dimensional matrix (7) are structured by (3 by 3) matrix as in (8).

$$w_i(x,y,1)=\begin{pmatrix} a_i & 0 & c_i \\ 0 & b_i & d_i \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix},\ \ i=1,2,...,N. \tag{8}$$

Then the 4-affine transformations in (7) are arranged in a (4 by 4) matrix in (9),

$$\mathrm{H}=\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix}. \tag{9}$$

We calculate the Hutchinson operator $W=w_4w_3w_2w_1$ and represent it in the form of (8), as in (10).

$$W(x,y,1)=\begin{pmatrix} A & 0 & C \\ 0 & B & D \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \tag{10}$$

where (10)

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

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.

Algorithm: This algorithm is a generalization of Guillou-Quisquater identification protocol using IFS transformations. It consists of two parts, the initialization and the identification.

Initialization: Initially the parameters (matrix H, g, p) must be agreed upon by the prover and the verifier, (where $g\in Z$ and p is prime number). We need to generate the number of iteration secretly in order to find the attractor of the IFS. This fractal attractor is used for generating the public keys and also for the proving and verifying processes. A Diffie-Hellman [26] key exchange protocol is used to generate this shared private key n.

- Generate numbers (x, s), (x',r) as receiver and signer of private keys, where $x,x'\in R$, $r,s\in Z$.
- Calculate $F_s=g^s \pmod p$, $F_r=g^r \pmod p$ as prover and verifier of public keys.
- Exchange F_s and F_r.
- After receiving F_r, the receiver calculates a private shared key $n=(F_s)^r \pmod p$, the number of iteration for the IFS and generates the fractal attractor W^n used in the cryptosystem,

$$W^n=\begin{pmatrix} A^n & 0 & \left(T_n(A)\right)C \\ 0 & B^n & \left(T_n(B)\right)D \\ 0 & 0 & 1 \end{pmatrix} \tag{11}$$

where, $T_n(A)=A^{n-1}+A^{n-2}+\ldots+A+1$ and
$T_n(B)= B^{n-1}+B^{n-2}+\ldots+B+1.$

Identification:

- Based on their private keys x, x' and using the fractal attractor W^n the prover and the verifier generate the public key $u = W^n(x,0,1)$ and $u' = W^n(x',0,1)$ then,

$$u = A^n x + T_n(A)C \text{ and}$$
$$u' = A^n x' + T_n(A)C$$

- Exchange (u) and (u') between them.
- The prover has the public key u' and the private key x and uses them to calculate $z'=\left(\frac{u'-T_n(A)C}{A^n}\right)*\mathrm{x}.$
- The verifier on the other hand has the public key u and the private key x' and uses them to calculate

$$z = \left(\frac{u - T_n(A)C}{A^n} \right) * x'.$$

- Now the prover uses z' and the fractal attractor W^n to find $v' = W^n(0,z',1)$ and sends it to the verifier where $v' = B^n z' + T_n(B)D$.
- The verifier after receiving the prover's key v', uses his private key z and the fractal attractor W^n to find $v = W^n(0,z,1)$, where $v = B^n z + T_n(B)D$ and compares with v'.
- If v=v', then the authentication succeeds.

RESULTS

In this section the implementation of GQ method and its generalization using fractal functions are discussed with two computer examples.

Software Implementation: The Guillou-Quisquater algorithm and its generalization using IFS, with its graphic user interface Figure (3,4), are carried out using Java under Net-Beans IDE 6.8. They are compared according to the time and key space parameters as performance parameters under the same environment. The efficiency of the algorithms is documented and analyzed in the next section. All the results were obtained using a computer with these specifications: 3.0GHz Intel (Cor.2 Duo) CPU and 2GB RAM.

Examples

Example 1: Figure (5) shows the executing results for GQ method using random data with 1024 bits.

Example 2: We use the IFS transformations as in (12).

$$H = \begin{pmatrix} 0.5 & 0.5 & 0 & 0 \\ 0.5 & 0.5 & 0 & 0.25 \\ 0.5 & 0.5 & 0.25 & 0 \\ 0.5 & 0.5 & 0.5 & 0.5 \end{pmatrix} \quad (12)$$

The fractal attractor of this affine transformation functions is illustrated in Figure (6) and the Hutchinson operator W is,

$$W = \begin{pmatrix} 0.0625 & 0 & 0.5 \\ 0 & 0.0625 & 0.3125 \\ 0 & 0 & 1 \end{pmatrix} \quad (13)$$

The data in Figure (7) is the executing result using random keys with 1024 bits.

Fig. 3: Fractal zero-knowledge user interface

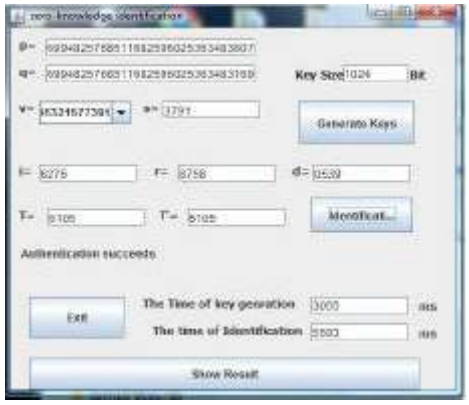


Fig. 4: Guillou-Quisquater user interface

Fig. 5: Executing results for GQ method

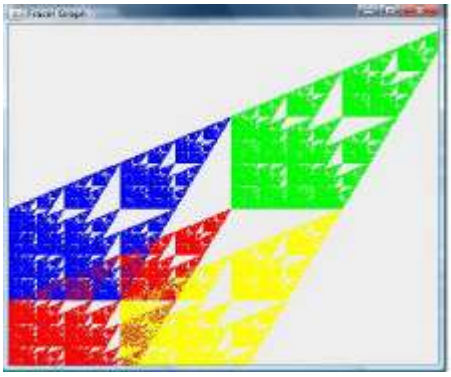
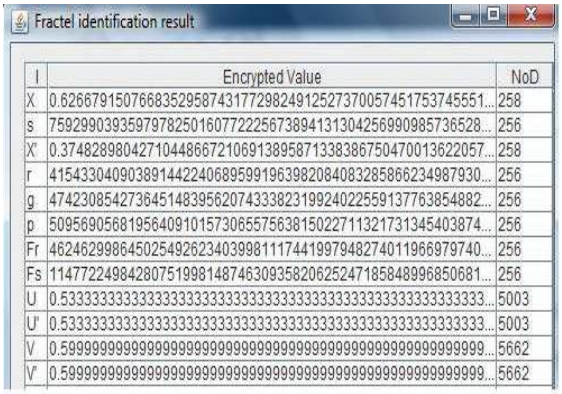


Fig. 6: Fractal Attractor for the given IFS



I	Encrypted Value	NoD
X	0.626679150766835295874317729824912527370057451753745551...	258
s	759299039359797825016077222567389413130425699098573652 8...	256
X'	0.374828980427104486672106913895871338386750470013622057...	258
r	415433040903891442240689599196398208408328586623498793 0...	256
g	474230854273645148395620743338231992402255913776385488 2...	256
p	509569056819564091015730655756381502271132173134540387 4...	256
Fr	462462998645025492623403998111744199794827401196697974 0...	256
Fs	114772249842807519981487463093582062524718584899685068 1...	256
U	0.533333333333333333333333333333333333333333333333333333...	5003
U'	0.533333333333333333333333333333333333333333333333333333...	5003
V	0.599999999999999999999999999999999999999999999999999999...	5662
V'	0.599999999999999999999999999999999999999999999999999999...	5662

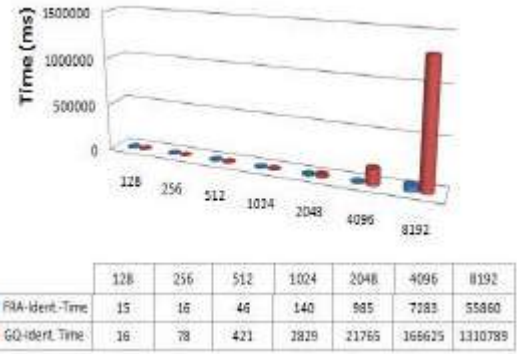
Fig. 7: Executing results for Fractal zero-knowledge protocol.

DISCUSSION

Design of efficient and secure identification mechanisms is a major research topic in data security. Modern cryptography is concerned with the implementation of cryptosystems that assure a sufficiently high level of security to prevent any attempt to foil the protection of information. Fractal cryptography is based on an NP-hard problem [14,27], which means that it cannot be solved within a reasonable period of time. So it could be considered as a useful tool in the design of secure systems.

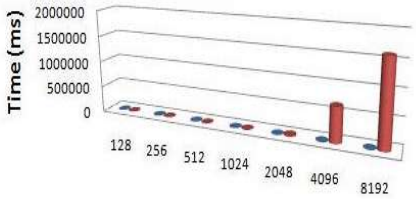
The proposed zero knowledge protocol based on IFS involves two parties, Peggy and Victor. Peggy tries to prove her identity to Victor without telling her private information (x,n). Then she generates a public key u, using the Hutchinson matrix W^n and sends it to Victor. On the other hand Victor has the same strategy and sends his public key u' to Peggy. Now Peggy uses the IFS and her private keys to compute V' and sends it to Victor. To verify Peggy's secret, Victor needs to compute V. If $V=V'$, then Victor can convince that Peggy knows the secret and the authentication process is deemed successful. Trying to find the private keys entails solving the equation with two unknowns which is computationally impossible. This will prevent attacks on private key values. If the number of bits is k, then there are 2^k possibilities for every value of x and n. In this case the brute force attack does not work when the length of these keys is as long as possible.

Using the same key size, performance comparison is accomplished between fractal zero-knowledge and Guillou-Quisquater for different key lengths. We conclude from their execution that fractal method perform better than GQ in terms of time and key size as shown in the Figures (8, 9) below.



	128	256	512	1024	2048	4096	8192
FRA-Ident.-Time	15	16	46	140	985	7283	55860
GQ-Ident. Time	16	78	421	2829	21765	166625	1310789

Fig. 8: Comparison of identification times



	128	256	512	1024	2048	4096	8192
FRA-Key-Gen. Time	0	16	16	47	140	407	1343
GQ-Key-Gen.Time	15	31	140	1047	18046	659125	1610754

Fig. 9: Comparison of key generation times

CONCLUSION

A novel fractal protocol is proposed in this paper to be used in zero-knowledge systems, provided all fractal functions are based on a continuous infinite interval (0,1) to ensure the satisfaction of the contraction property and create a massive search space. Another important fact is the security of fractal cryptography functions, which is based on NP-hard problem, to ensure it cannot be solved within a reasonable period of time. 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 protocol and the GQ protocol, we conclude that zero knowledge systems based on IFS transformation perform more efficiently than GQ system in terms of key size and key space.

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.

REFRENCES

1. Berson, T., S. Guillou, G. Guillou, A. Guillou, G. Guillou, M. Guillou, L. Guillou, Mi. Quisquater, Mu. Quisquater, My. Quisquater and J. Quisquater, 1990. How to explain zero-knowledge protocols to your children. In: Advances in Cryptology- CRYPTO 89, G. Brassard, editor, Santa Barbara, California, USA, August 20-24, 1989, pp: 628-631.
2. Sharma, A. and D. Brat Ojha. 2010. "Application of Coding Theory in Fuzzy Commitment Scheme". Middle-East J. Scientific Res., 5(6): 445-448.
3. Menezes, A.J., P.C.V. Oorschot and S.A Vanstone, 1997. Handbook of Applied Cryptography, Boca Raton, CRC Press.
4. Al-Momani I., M. Al-Saruri and M. Al-Akhras, 2011. "Secure Public Exchange Against Man in the Middle Attacks During Secure Simple Pairing (SSP) in Bluetooth. World Applied Sciences J., 13(4): 769-780.
5. Goldwasser, S., S. Micali and C. Rckoff, 1989. The Knowledge Complexity of Interactive Proof Systems, SIAM J. Computing, 18: 186-208.
6. Goldreich, Micali and Wigderson Proofs that Yield Nothing but their Validity or All Languages in NP have Zero-Knowledge Proofs. JACM, July 1991.
7. A. Fiat and A. Shamir, 1987. How to Prove Yourself: Practical Solutions to Identification and Signature Problem, Crypto, 86(263): 186-189.
8. Micali, S. and A. Shamir, 1988. An Improvement of the Fiat-Shamir Identification and Signature Scheme, Crypto, 88(403): 244-250,1988.
9. Fiege, U., A. Fiat and A. Shamir, 1987. Zero Knowledge Proof of Identity, Proc. of 19th STOC, pp: 210-217.
10. Guillou, L.C. and J.J. Quisquater, A. Paradoxical Identity-Based Signature Resulting From Zero Knowledge, Crypto, 88(403): 216-231, 1988.
11. Shafi Goldwasser, 1991. Yael Tauman Kalai: On the (In)security of the Fiat-Shamir Paradigm. FOCS 2003: 102-107, 2003. 38(1): 691-729.
12. Courtois, N.T., 2001. Efficient Zero-Knowledge Authentication Based on a Linear Algebra Problem MinRank , Asiacrypt, 2248: 402-411.
13. Wolf, C., 2004. Zero-Knowledge and Multivariate Quadratic Equations, Workshop on Coding and Cryptography.
14. Alia, M. and A. Samsudin, 2008. Fractal (Mandelbrot and Julia) Zero-Knowledge Proof of Identity. J. Computer Sci., 4(5): 408-414.
15. Shuichi Aono† and Yoshifumi Nishio, 2007. A User Authentication Protocol Using Chaotic Maps. RISP International Workshop on Nonlinear Circuits and Signal Processing (NCSP'07).
16. Barnsley, M.F. and S. Demko, 1985. Iterated function systems and the global construction of fractals, Proc. Roy. Soc. London A399: 243-275.
17. Hutchinson, J., 1981. Fractals and self-similarity. Indiana University Mathematics J., 30(5): 713-747.
18. Barnsley, M., 1993. Fractals Everywhere. Academic Press Professional, Inc. San Diego, CA, USA, Second Edition.
19. Nikiel, S., 2007. Iterated Function Systems for Real-Time Image Synthesis, Springer-Verlag London Limited.
20. Fisher, Y., 1995. Fractal Image Compression: theory and application. Springer-Verlag. New York, USA.
21. Dugelay, J.L., E. Polidori and S. Roche, 1996. Iterated Function Systems for Still Image Processing. IWISP-96, Manchester, UK, November. Indian Institute of Technology Bombay. Mumbai.
22. Jacquin, A.E., 1992, Image coding based on a fractal theory of iterated contractive image transformations. EEE Trans. Image Processing, 1(1): 18-30.
23. Goldreich, O. and Y. Oren, 1994. Definitions and Properties of Zero-Knowledge Proof Systems, J. Cryptol., 7(1): 1-32.
24. Goldreich, O., 2002. Zero Knowledge Twenty Years after its Invention, Electronic Colloquium on Computational Complexity, Technical Report TR02-063.
25. Guillou, L.C. and J.J. Quisquater, 1988. "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory," Advances in Cryptology-EUROCRYPT '88 Proceedings, Springer-Verlag, pp: 123-128.
26. Diffie, W. and M.E. Hellman, 1976. New Directions in Cryptography, IEEE Transaction on Information Theory, 22(6): 644-654.
27. Massopust, P.R., 1997. Fractal Functions and their Applications, Chaos, Solitons and Fractal, 8(2): 171-190.