Signature Identification Scheme Based on Iterated Function Systems

Nadia M. G. AL-Saidi

***Abstract*—**Since 1984 many schemes have been proposed for digital signature protocol, among them those that based on discrete log and factorizations. However a new identification scheme based on iterated function (IFS) systems are proposed and proved to be more efficient. In this study the proposed identification scheme is transformed into a digital signature scheme by using a one way hash function. It is a generalization of the GQ signature schemes. The attractor of the IFS is used to obtain public key from a private one, and in the encryption and decryption of a hash function. Our aim is to provide techniques and tools which may be useful towards developing cryptographic protocols. Comparisons between the proposed scheme and fractal digital signature scheme based on RSA setting, as well as, with the conventional Guillou-Quisquater signature, and RSA signature schemes is performed to prove that, the proposed scheme is efficient and with high performance.

***Keywords*—**Digital signature, Fractal, Iterated function systems (IFS), Guillou-Quisquater (GQ) protocol, Zero-knowledge (ZK)

I. INTRODUCTION

SUBSEQUENT to the appearance of the first idea of a digital signature that relied on public key algorithms, many novel schemes were introduced and many new properties added. A ZK proof of identity is a novel idea in the identification schemes that relied on public key algorithms. It is cryptographic protocols provides provably secure entity authentication, without revealing any knowledge to any entity or to any eavesdropper based on hard computational problem.

Secure identification is an important security affair to avoid computer fast developments. Using a hash function, a secure digital signature scheme can be constructed. A digital signature scheme has equal complexity as the identification scheme [1]. It is used to build effective communication tools and to ensure privacy. The ZK protocol was proposed at first as a method for exchanging public keys, for creating digital signatures or for protecting digital cash on smart cards. It is considered as time-consuming than other authentication methods, but also harder to crack [2]. The identification protocol by GQ is a particular type of digital signature defined in an RSA setting, but generates its own signature, which is vulnerable compared to the digital signature generated by RSA scheme. The concept of a digital signature was introduced by Diffie and Hellman in1976. They published their landmark paper”New Directions in Cryptography” [3]. The RSA signature is the first method discovered and it is approved as a standard system and is popular and most widely used.

The signature works in Z_n where n is the product of two large primes’ p and q, and its security is based on the hardness of the modeling and factorization problem. The ZK Proof was first introduced by Goldwasser, Micali and Rackoff [4] in 1985. The wide applicability of ZK was demonstrated by Goldreich, Micali and Wigderson in [5]. Fiat and Shamir [6] introduced an identification and signature scheme that helps to prove the identity and the authenticity of the messages. The system generate signature which is vulnerable compared to the digital signature generated by the RSA scheme. Guillou and Quisquater (GQ) presented an identification and signature scheme [7]. It is an extension of the RSA protocol which reduces the number of rounds needed to 1, and its security is based on intractability of RSA problem.

Unlike the identification and signature scheme of previous studies which based on factorization problem or discrete logarithm problem on a finite field, new systems for identification and signature based on infinite fields pose as new challenges in modern cryptosystems. Alia, M. and A. Samsudin in [8] proposed a new ZK proof of identity protocol based on Mandelbrot and Julia Fractal sets. They identified that the security of the proposed fractal ZK proof of identity is based on the NP-hard problem and the randomness of the output generated. Shuichi Aono, Yoshifumi Nishio, in [1] proposed an authentication protocol by using of three times the authentication interaction. This authentication protocol is based on iterations of the logistic map in public-key cryptography. Al-Saidi N. and Rushdan M. in [9] proposed a new digital signature scheme based on IFS. They generate the new digital signature system, based on fractal attractor.The remaining sections of this paper are organized as follows. The mathematical preliminaries about the iterated function system are presented in the materials and methods section. Following this the concepts of digital signature schemes, and GQ signature are summarized. A new digital signature identification scheme, based on IFS as a generalization of (GQ) identification and signature schemes is proposed. An example, and the performance analysis, are analyzed in the results and discussions section. Finally conclusions are drawn.

II. MATERIALS AND METHODS

A- Iterated Function Systems

The term “iterated function system” (abbreviated: IFS) was coined in [10] by Barnsley & Demko to describe a general framework of dynamics. However, most of the results about the IFS model are presented in [11]-[12]. This section provides an overview of the major concepts and results of Iterated Function System (IFS) and their

Nadia M.G. Al-Saidi is with Applied Sciences Department-Applied Mathematics University of Technology -Baghdad-Iraq.e-mail: nadiamg08@gmail.com

application. A more detailed review of the topics in this section are as in [13]-[14].

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,

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

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

Definition 3. An (hyperbolic) iterated function system is a couple (X, w), where $w=\{w_i\}, i=1,\ldots N$, such that $w_i{:}X\rightarrow X$, which are contractions of contractivity factors $s_i\in[1,0)$ with respect to the metric d.

An IFS describes a unique set: it is the attractor. The attractor is an 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, such a set is always exists. It first appeared in Hutchinson [11].

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 $w{:}X\rightarrow X$ 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 $\lim_{n\to\infty} w^{\circ n}(x)=x_f$, where $w^{\circ n}$ is the n-fold composition of w.

Definition 3. Any affine transformation $w{:}R^2\rightarrow R^2$ of the plane has the form,

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

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

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,

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

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.

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

B- Signature Identification.

A digital signature (DS) is performed by three algorithms (key generation, signing and verification). It is a polynomial-time algorithms [15].

- Key Generation. On input k, where k denotes the security parameter, the algorithm produces a pair of matching public and secret keys (p_k, s_k).
- Signing. On input (s_k,m), the algorithm returns a signature $\sigma = \text{Sign}_{sk}(m)$, where m is a message.
- Verification. On input (p_k,m, σ), the algorithm returns 1 (accept) or 0 (reject). It is required that $\text{Verify}_{pk}(m,\sigma)=1$, for all $\sigma \leftarrow \text{Sign}_{sk}(m)$.

C- Guillou-Quisquater Signature Scheme.

The GQ signature scheme is a modification of the GQ identification protocol obtained by replacing the challenge with a one-way hash function *SHA-1*. The signing key J and the verification key B are related via $JB^v=1$. The three components of the GQ signature are presented as follows [16].

1. Key generation: The signer generates two primes p and q $(n=pq)$, and chooses a prime e as the public exponent in the RSA setting. Then computes $d = e^{-1} \pmod{\varphi(n)}$, chooses a random number $J\in Z^n$ and computes the signing key $s = (1/J)^d \pmod{n}$. He then publishes the verification key set $V_K = (n, e, J, SHA\text{-}1)$, where *SHA-1* is a hash function, $SHA\text{-}1{:}\{0, 1\}^* \rightarrow Z_n^*$. The signing key B and the system secret for the signer d, are kept secret separately.
2. Signature generation: The signer chooses a random number $r\in Z_n^*$ and computes $s= SHA\text{-}1(r^e \parallel M)$ and $z= rB^a$. The signature pair is (s, z).
3. Signature verification: Upon receiving (s,z), the verifier computes $s' = SHA\text{-}1(z^e J^a \parallel M)$.

The signature is accepted if $a=a'$.

In this scheme, only someone with knowledge of B can successfully forge the signature. Given arbitrary J, to compute B, the e-th root of $1/J$ is the inverse RSA problem, which is assumed to be intractable.

D- Using Fractal to Generalize GQ- Identification Protocol.

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, translation, and scaling. These equations can generate complicated fractal images [17]. An explanation is given here on how to get GQ signature from GQ identification based on iterated function system.

The Fractal method [9]: To generate fractal attractor, the Hutchinson operator W is constructed based on a given affine transformation. Consider an IFS consisting of the maps,

$$w_i(x,y)=\begin{pmatrix} a_i & 0 \\ 0 & d_i \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}+\begin{pmatrix} c_i \\ d_i \end{pmatrix},\ i=1,2,\ldots,N. \qquad (5)$$

Fractal generated using IFS of four affine transformation (w_1,w_2,w_3,w_4) are used and arranged in a matrix H, where the generalized case can be easily followed. The affine transformation given by (5), satisfy the semi-group property.

A dummy coordinate Z with value 1 is added to represent the translation in the affine transformation, and the 2-dimensional matrix (5) are structured by (3 by 3) matrix as in (6).

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

We calculate the Hutchinson operator W=$w_4w_3w_2w_1$, and represent it in the form of (6), then we have (7).

$$W=\begin{pmatrix} A & 0 & C \\ 0 & B & D \\ 0 & 0 & 1 \end{pmatrix},\text{where} \qquad (7)$$

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

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

The Algorithm

The fractal identification protocol can be turned into a digital signature mechanism by using a one way hash function SHA-1: $\{0,1\}^* \rightarrow Z_n^*$. It consists of two parts, key generation, and signature protocol.

1- Key Generation

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 to find the attractor of the IFS, which is used for generating the public key and for signing and verifying process. A Diffie-Hellman key exchange protocol is used to generate this secret private key n.

Each entity has to create a public key and a corresponding private key.

a- Entities A & B generate the numbers (x, s), (x',r) as private keys, where $x,x'\in R$, $r,s\in Z$.

b- Calculate $F_s=g^s \pmod p$, $F_r=g^r \pmod p$ as public keys.

c- Exchange F_s, and F_r.

d- After receiving F_r, entity A 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 to be used in the cryptosystem,

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

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

e- Based on their private keys x, x', and using the fractal attractor W^n entities A & B generate the public keys $u = W^n(x,0,1)$, and $u' = W^n(x',0,1)$, where
$u = A^n x + T_n(A)C$, and
$u' = A^n x' + T_n(A)C$

f- Exchange (u) and (u') between them.

2- Signature Protocol

Entity A signs a message M. Any entity B can verify this signature by using A's public key.

Signature generation: Entity A should do the following:

a- Determine the message to be signed and represent it as pairs M=(m_1;m_2).

b- Calculate $z=\left(\frac{u'-T_n(A)C}{A^n}\right)*x.$ using the public key u' and the private key x.

c- Use z and the fractal attractor W^n to find $v'=W^n(0,z,1)$, where $v'= B^n z + T_n(B)D$.

d- Then the hash function *SHA-1* is used to generate the signature s'=*SHA-1*(M,v') and send s' with the message M to entity B.

Verification: To verify A's signature s' on M, Entity B should do the following:

e- Use the public key u and his private key x' to calculate $z'=\left(\frac{u-T_n(A)C}{A^n}\right)*x'.$

f- After receiving (M,s') the verifier generate the signature s=*SHA-1*(M,v), where $v=W^n(0,z',1)$ is calculated using the private key z' and the fractal attractor W^n, such that $v = B^n z'+T_n(B)D$.

g- Compare if $s=s'$, then the signature has been verified.

III. RESULTS AND DISCUSSION

The algorithm for the proposed protocol in this paper is formalized based on nonlinear fractal function (IFS), that is defined within the infinite subfield (0,1). All the algorithms 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 by direct input text. The efficiency of the algorithms is documented in this section. All the results have been obtained using a computer with the specifications: 3.0GHz Intel Cor. 2 Duo CPU, and 2GB RAM.

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

$$H=\begin{pmatrix} 0.5 & 0.5 & 0 & 0 \\ 0.5 & 0.5 & 0.25 & 0.25 \\ 0.5 & 0.5 & 0.25 & 0.25 \\ 0.5 & 0.5 & 0.5 & 0 \end{pmatrix}. \qquad (6)$$

Fractal attractor of this affine transformation function is illustrated in Fig.1, it is a known fractal example called Sierpinski Triangle. The Hutchinson operator W is given in (7)

$$W=\begin{pmatrix} 0.0625 & 0 & 0.6875 \\ 0 & 0.0625 & 0.1875 \\ 0 & 0 & 1 \end{pmatrix}. \qquad (7)$$

Sierpinski Triangle is used to carry out the fractal digital signature protocols with different key size as illustrated in Table I.

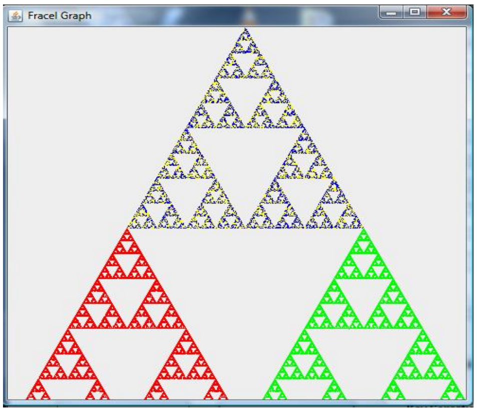


Fig. 1 Fractal attractor for the given IFS

A- Performance Analysis

The fractal protocols is able to withstand the known attacks. They are considered as time consuming to be involved in solving non-linear system of equations numerically over the aforementioned infinite subfield. Hence the attempts to recover the private key using the trial and error methods seems to be computationally not feasible, even if the attacker can access some secret parameters, because they are generated randomly. However, due to the open key space and big key size, the search space is massive, and the cumulative and truncation errors that accompany all numerical solutions of non-linear system of equation pose some strength to the proposed algorithm to obtain imprecise decimal numbers. Some additional random values are introduced to the algorithm, that could help to ensure a large number of unknowns over number of equations to secrete the values of ciphertext through transmission. These added noise is removed after decrypting using their inverses. Hence, many well known attacks fail to solve the system of equation and find the imprecise secret key parameter from the given public one. The one way property of the authenticated value (Hash function *SHA-1*) increases the insurance that the message cannot be recovered easily, so it is considered as a factor to strengthen the security of the protocol.To prevent the brute force attack, the choice of the key size becomes a crucial issue. The key space depends on the size of the key. For any chosen number of bits (n), the fractal key space includes 2^n possible key values, while the number of possible keys for RSA and GQ is limited to the number of primes in Z_p where p is the largest n-bits prime. The estimated value of RSA key space is calculated by n=log n, where key space is another factor play the main role in the security of digital signature protocol, to ensure the hardness of the problem and to prevent some known attacks.The performance comparison of the proposed protocol among fractal digital signature protocol [9], is done in terms of execution time and key size, as shown by Table I. Also among two another digital signature protocols based on finite field that deals with discrete log and factorization problem, which are GQ, and RSA digital signatures. We found that, as explained in Table I, the fractal digital signature based identification performs better than fractal digital signature based RSA in term of key generating time, but the latest performs better in term of the signature and verification times. The first value in each column in Table I, represent the key generation time and the second value is the sum of the signature and the verification time. From the same table, we conclude that GQ digital signature scheme perform better than RSA digital signature schemes in terms of the same parameters and under the same environment. The resulted values for different key size in Table. I is graphed in Fig.(2,3).

IV. CONCLUSIONS

Based on nonlinear fractal functions defined within the infinite subfield (0,1), a new digital signature protocol is proposed in this paper. The main purpose for investigating into this study is to find a system which perform better than what exist currently. Also using the fact that fractal functions was proved as an NP-Hard problem, is to ensure it cannot be solved in practical amount 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 digital signature protocols and the counterpart public protocols, such as RSA and GQ digital signatures, we conclude that, the proposed schemes based on fractal functions resulted in a better performance compared to the counterpart schemes in terms of the evaluation parameters, key space, and key size.

REFERENCES

[1] Shuichi Aono†, Yoshifumi Nishio, 2007. A User Authentication Protocol Using Chaotic Maps. RISP International Workshop on Nonlinear Circuits and Signal Processing (NCSP'07), pp 333-336.

[2] Menezes A.J., Oorschot P.C.V., Vanstone S.A , 1997. Handbook of Applied Cryptography, Boca Raton, CRC Press.

[3] Diffie W. and Hellman M. E., 1976. New Directions in Cryptography. IEEE Transactions on Information Theory, IT-22: 644–654.

[4] Goldwasser S., Micali S., and Rckoff C., 1989. The Knowledge Complexity of Interactive Proof Systems, SIAM journal of computing, 18: 186-208.

[5] Goldreich, Micali and Wigderson, 1991. Proofs that Yield Nothing But their Validity or All Languages in NP have Zero-Knowledge Proofs. Journal of the Association for Computing Machinery, 38(1): 691-729.

[6] Fiat A. and Shamir A., 1987. How to Prove Yourself: Practical Solutions to Identification and Signature Problem, Crypto 86, 263: 186-189.

[7] Guillou L.C. and Quisquater J.–J., 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.

[8] Alia, M. and Samsudin A., 2008. Fractal (Mandelbrot and Julia) Zero-Knowledge Proof of Identity. Journal of Computer Science 4(5): 408-414.

[9] AL-Saidi, N.and Said, M.R.Md., 2010. Fractal attractor based digital signature. Sixth International Conference on Networked Computing and Advanced Information Management (NCM), pp: 446 – 449.

[10] Barnsley M.F. and Demko S., 1985. Iterated function systems and the global construction of fractals, Proc. Roy. Soc. London A399, 243-275.

[11] Hutchinson J., 1981. Fractals and self-similarity. Indiana University Mathematics Journal 30(5): 713–747.

[12] Hart J.C., 1991. Computer Display of Linear Fractal Surfaces. Ph.D. Dissertation, EECS. Dept., university of Illinois at Chicago, Sept.

[13] Barnsley M., 1993. Fractals Everywhere. Academic Press Professional, Inc., San Diego, CA, USA, second edition.

[14] Massopust P. R., 1997. Fractal Functions and their Applications, Chaos, Solitons and Fractal 8(2): 171-190.

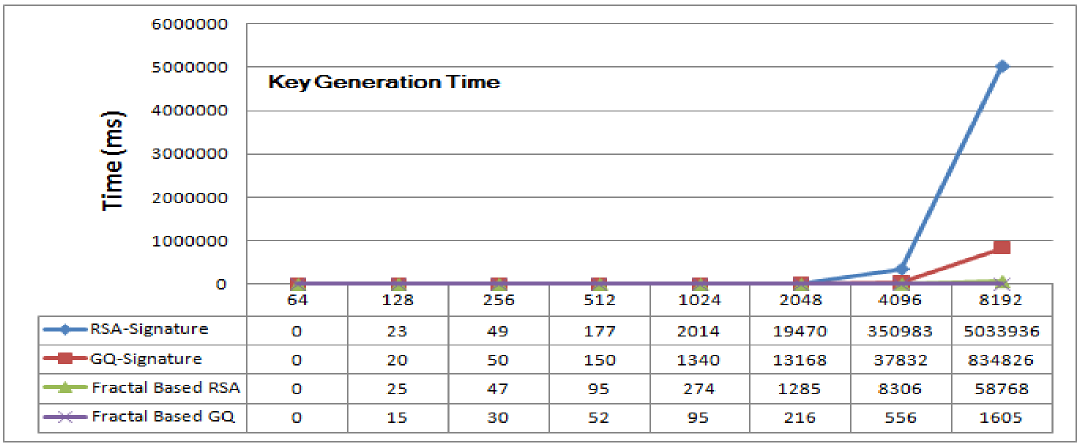
[15] Kurosawa K., Heng S.H., 2004. From Digital Signature to ID-based Identification/Signature. In Proceedings of Public Key Cryptography, pp.248-261.

[16] Cheng F.LU and Shiuhpyng Shien, 2001. Efficient key-Evolving Protocol for the GQ Signature. Journal of Information Science and Engineering 20: 763-769.

[17] Guojun L. and Toon L. Y.,1996, Applications of Partitioned Iterated Function Systems in Image and Video Compression. Journal of Visual Communication and Image Representation. 7(2): 144-154.

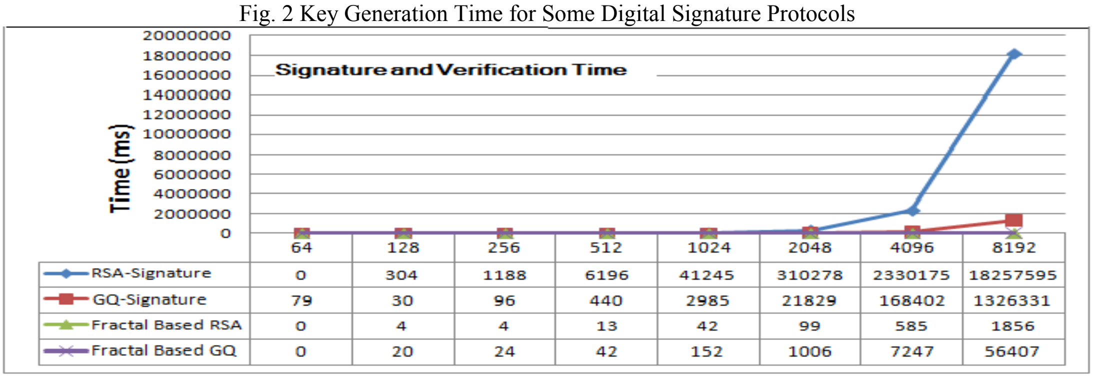
TABLE I
PERFORMANCE COMPARISION FOR SOME DIGITAL SIGNATURE PROTOCOLS

	Fractal Based GQ	Fractal Based RSA	GQ-Signature	RSA-Signature
No. of Bits	Key Gen. Time-- Sig.&Ver. Time	Key Gen. Time -- Sig.&Ver. Time	Key Gen. Time -- Sig.&Ver. Time	Key Gen. Time -- Sig.&Ver. Time
128	15-20	25-4	20-30	23-304
256	30-24	47-4	50-96	49-1188
512	52-42	95-13	150-440	177-6196
1024	95-152	274-42	1340-2985	2014-41245
2048	216-1006	1285-99	13168-21829	19470-310278
4096	556-7247	8306-586	37832-168402	350983-2330175
8192	1605-56407	58768-1856	834826-1326331	5033936-18257595



	64	128	256	512	1024	2048	4096	8192
RSA-Signature	0	23	49	177	2014	19470	350983	5033936
GQ-Signature	0	20	50	150	1340	13168	37832	834826
Fractal Based RSA	0	25	47	95	274	1285	8306	58768
Fractal Based GQ	0	15	30	52	95	216	556	1605

Fig. 2 Key Generation Time for Some Digital Signature Protocols



	64	128	256	512	1024	2048	4096	8192
RSA-Signature	0	304	1188	6196	41245	310278	2330175	18257595
GQ-Signature	79	30	96	440	2985	21829	168402	1326331
Fractal Based RSA	0	4	4	13	42	99	585	1856
Fractal Based GQ	0	20	24	42	152	1006	7247	56407

Fig. 3 Signature and Verification Time for Some Digital Signature Protocols