Int. Journal of Math. Analysis, Vol. 5, 2011, no. 29, 1399 - 1410

On the Security of Digital Signature Protocol Based on Iterated Function Systems

Nadia M. G. AL-Saidi [1] **and Mohamad Rushdan Md. Said**

Institute for Mathematical Research (INSPEM)
Universiti Putra Malaysia
43400 Serdang, Selangor, Malaysia

Abstract

A common goal of cryptographic research is to design protocols that provide a confidential and authenticated transmission channel for messages over an insecure network. Hash functions are used within digital signature schemes to provide data integrity for cryptographic applications. In this paper, we take a closer look at the security and efficiency of the digital signature protocol based on fractal maps. This new system can be expected to have at least the same computational security against some known attacks. A Diffie-Hellman algorithm is used to improve the security of the proposed protocol by generating the number of iteration that is used to find the attractor of the iterated function system, which is used to calculate the public key and the signature. The proposed algorithm possesses sufficient security against some known attacks applicable on finite field cryptosystems. They are considered as time consuming to be involved in solving non-linear systems numerically over the defined infinite subfield.

Mathematics Subject Classification: 81Q, 94A

Keywords: Fractal, Iterated Function Systems (IFS), Attractor, Fractal Digital Signature Algorithm (FDSA)

1 Introduction

Cryptography is the study of mathematical and computational techniques related to the aspects of information security. The fundamental security requirement for certified encryption is privacy of encrypted data. The prove of the difficulty of the algorithms is summarized under the category of mathematical

[1] nadia_alsaidi@hotmail.com

problems. Designing cryptographic protocols is a very challenging problem. In open networks, such as the Internet, protocols should work even under worst-case assumptions, namely messages may be eavesdropped or tampered with by an attacker (also called the intruder or adversary)[18].

Digital signatures are strong tools applied to achieve the security services of authentication (proof of identity of the sender), data integrity (detection of changes to the message) and non-repudiation (prevention of denial of sending the information).They are digital counterparts of handwritten signatures that can be transmitted over a computer network [4]. Only the sender makes the signature, and other people can easily recognize it as belonging to the sender. The concept of a digital signature was introduced in 1976 by Diffie and Hellman. They published their landmark paper "New Directions in Cryptography" [21].

Due to their complicated mathematical structure and deterministic nature, especially their recursive construction, fractal functions have many applications in applied sciences. The latest applications of certain elements of fractal geometry, namely the aforementioned fractal function are in the cryptographic systems. It has the potential to create a new way of securing important information to be transmitted or stored. Also due to its pseudo random nature, many statistical cryptanalysis methods cannot be applied [15]. 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. For details on the relation between chaos and fractals, refer to [8, 10].

Many studies on chaos-based cryptosystems and fractal based Cryptosystems have been published. Much work has been done by incorporating chaotic maps into the design of symmetric and asymmetric encryption schemes. In 2003, Kocarev and Tasev[9] proposed a public key encryption algorithm based on Chebyshev chaotic maps. Since then many studies that proposed new protocols based on chaotic maps have been carried out. In 2005, Gonzalo [1] proposed a new scheme making use of a chaos-based encryption hash parallel algorithm and the semi-group property of the Chebyshev chaotic map, for deniable authentication. In 2007, Xiao et al. and Deng [22] proposed an original key agreement protocol based on Chebyshiv maps, and in 2008, Yoon and Yoo [7] proposed a new key agreement protocol based on chaotic maps that can reduce the number of communication rounds [20]. Also, some work incorporating the fractal functions into the design of symmetric and asymmetric encryption schemes using the similar mechanism have been proposed in [5, 6, 12, 13, 17].

Although many of the proposed schemes have several advantages, such as computational efficiency and ease of generating public-private key pairs, they fail to explain a number of features that are fundamentally important to all kind of cryptosystems. The outline of this paper is as follows. In Section 2, some theoretical Background and the main concepts are given. In Section 3, the proposed protocol for the application of fractal function in digital signature systems is presented, with the algorithm. In section 4, the security of fractal digital signature scheme that proposed in [13] is analyzed with respect to the security goals of privacy and authenticity. Section 5 concludes the paper by discussing alternate and additional security goals that are not covered by in the previous sections, that may still be of interest.

2 Theoretical Background

In this section an overview of the major concepts are presented. A detailed review of the topics in this paper are given in [4, 10, 11, 19]. The theory of fractal sets is a modern domain of research. Iterated function systems have been used to define fractals [3].

Definition 2.1. Iterated Function System(IFS):
A hyperbolic IFS $\{X; w_1, w_2, ..., w_n\}$ consists of a complete metric space (X, d) and a finite set of strictly contractive transformation $w_n : X \to X$ with contractivity factors s_n, for $n = 1, ..., N$. The maximum s among $s_1, ..., s_N$ is called a contractivity factor for the IFS. The unique fixed point in $H(X)$ of the transformation W is called the *attractor* of the IFS.

Definition 2.2. Digital signature:
A digital signature scheme is a set of three algorithms [4]:

1. Key generation
   Input: security parameter κ
   Output: key pair (p_k, s_k)

2. Signing
   Input: signing key s_k, message m [and random r]
   Output: $\sigma = S(sk, m[, r])$

3. Verification
   Input: verification key p_k, signature σ [and message m]
   Output: $V(p_k, \sigma[, m]) = 0$ or 1

Definition 2.3. Hash Function:
The algorithm that transforms a message of any length to a string of a fixed length is called the message digest. A message-digest algorithm is a cryptographic hash algorithm (also known as a message digest algorithms, a one-way

function, or simply a hash function). It is computationally not feasible to find two messages with the same signature or to find the signature of a given message without knowledge of the private key[16]. The reasons for applying a digital signature in cryptosystems are to satisfy the Authentication and Integrity.

Definition 2.4. Authentication: Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user.

Definition 2.4. Integrity: In many scenarios, the sender and receiver of a message may need to be confident that the message has not been altered during transmission.

3 Digital Signature Protocol Based on IFS

The use of fractal has an advantage as only a few parameters would have to be stored. When used it as an encryption key it will be very robust to attacks. Even if the attacker managed to obtain parts of the key (or almost the entire key), but a small digit is missing or is incorrect, the fractal image is changed dramatically. In this case the attacker has no way to extrapolate the rest of the key. The second reason, the brute force attack will not work since a fractal key is time consuming to generate especially at high zoon levels [22]. There are many previous works in fractal cryptography. Most of these protocols were designed in symmetric approaches. In the proposed scheme [13], fractal is used to design digital signature system based on IFS transformations. The proposed protocol consists of, initialization, signing, extraction, and verification parts. The typical implementation of digital signature involves a message-digest algorithm and a public-key algorithm for encrypting the message digest through a message-digest encryption algorithm.

3.1 The Methodology

Consider an IFS consisting of the maps,[13]

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

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

$$\begin{pmatrix} a_1, b_1, c_1, d_1, e_1, f_1 \\ a_2, b_2, c_2, d_2, e_2, f_2 \\ \\ \\ a_N, b_N, c_N, d_N, e_N, f_N \end{pmatrix} \tag{2}$$

To explain our method, fractal generated using IFS of four affine transformation (w_1, w_2, w_3, w_4) are used, so that the generalized case may be easily followed. To ensure satisfaction of the semi-group property, we need to use fractals generated by affine transformation of the form:

$$w_i \begin{pmatrix} x, y \end{pmatrix} = \begin{pmatrix} a_i & 0 \\ 0 & d_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} c_i \\ d_i \end{pmatrix}, \quad i = 1, 2, ..., N. \tag{3}$$

Affine transformation as metric: when 2-dimensional matrices are not enough to represent an affine transformation by itself, because it cannot represent translation. The trick is to add a dummy Z coordinate, which always has the value 1, and then we can structure it into 3 by 3 matrix as,

$$w_i \begin{pmatrix} x, y, 1 \end{pmatrix} = \begin{pmatrix} a_i & 0 & c_i \\ 0 & b_i & d_i \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}. \tag{4}$$

Then the 4-affine transformations in (3) can be arranged in 4 by 4 matrix as:

$$H = \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix}. \tag{5}$$

Calculate the Hutchinson operator $W = w_4 w_3 w_2 w_1$, and arrange as (4) we have,

$$W = \begin{pmatrix} A & 0 & C \\ 0 & B & D \\ 0 & 0 & 1 \end{pmatrix}, \tag{6}$$

$A = a_4 a_3 a_2 a_1$, $A \neq 1$.
$B = b_4 b_3 b_2 b_1$, $B \neq 1$,
$C = a_4 a_3 a_2 c_1 + a_4 a_3 c_2 + a_4 c_3 + c_4$.
$D = b_4 b_3 b_2 d_1 + b_4 b_3 d_2 + b_4 d_3 + d_4$.

3.2 Fractal Digital signature Algorithm(FDSA)

A Hybrid cryptosystem between fractal and one of the key exchange protocols are used to generate a shared private key that is used as the number of iteration to generate the fractal attractor. The fractal protocol consists of three parts.

1. Initialization part

   Initially the parameters (matrix H, g, p) must be agreed upon by the signer and the receiver, (where $g \in Z$, and p is prime number). In order to sign the message using IFS transformation, we need to generate the attractor of the IFS. This can only done after generating the number of iterations secretly between them. The Diffie hellman (DH) key exchange protocols is used to generate this shared private key n that represents the number of iterations.

   a- Generate numbers (x, y, s), (x', y', r) as receiver, and signer's private keys, where $x, y, x', y' \in R$, and $r, s \in Z$.

   b- Calculate $F_s = g^s \pmod p$, $F_r = g^r \pmod p$ as receiver, and signer's public key.

   c- Exchange F_s, and F_r.

   d- 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 that is used in calculating the public key and the signature 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, $T_n(A) = A^{n-1} + A^{n-2} + \ + A + 1$, and $T_n(B) = B^{n-1} + B^{n-2} + \ + B + 1$.

   e- Using W^n to find the receiver and signer's public key $(u, v, 1) = W^n(x, y, 1)$, and $(u', v', 1) = W^n(x', y', 1)$ respectively, where $u = A^n x + T_n(A)C, \quad u' = A^n x' + T_n(A)C$, and
   $v = B^n y + T_n(B)D, \quad v' = B^n y' + T_n(B)D$

   f- Exchange (u, v) and (u', v').

2. Signature part

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

b- To guarantee the integrity of the message M, we use a one-way hash function which is easy to calculate but is impossible to invert using fundamental information theory.

c- Get the SHA-1 Hash algorithm to find $HM = (Hm_1, Hm_2)$=SHA(M)

d- The signer signed the message using his private key (x', y'), and the fractal attractor W^n and give $S = (s_1, s_2, 1) = W^n(Hm_1ux', Hm_2vy', 1)$.

e- Send (S, M) to the receiver.

3. Extraction and Verification Part

Choosing H as in (5) ensures that W^n is commute under composition, so due to this semi-group property, if $S = W^nM$, it follows that $M = W^{-n}S$.

a- After receiving (S, M), the receiver use SHA-1 to find $HM = (Hm_1, Hm_2) = SHA(M)$.

b- The receiver uses his private key (x, y) and the fractal attractor W^n to recover the message

$$M(m_1, m_2) = \left(\frac{s_1 - T_n(A)C}{(A^n x + T_n(A)C)(u' - T_n(A)C)}, \frac{s_2 - T_n(B)D}{(B^n y + T_n(B)D)(v' - T_n(B)D)}\right)$$

c- If $HM = M$, then the message is verified.

4 Cryptanalysis of FDSA

Cryptanalysis is the study of methods for obtaining the meaning of encrypted information without accessing the secret information To prevent security attacks, there are five security goals we have to satisfy: data confidentiality (keeping information secret from unauthorized access), data integrity (integrity means that changes should be done only by authorized users and through authorized mechanisms.), authentication (both the sender and receiver need to confirm the identity of other party involved in the communication), non-repudiation (an entity is prevented from denying its previous commitments or actions) and access control (an entity cannot access any entity that it is not authorized to). The idea of digital signatures can provides message integrity, message authentication and non-repudiation. We can divide attacks roughly into two classes: passive attack and active attack.

A passive attack is one in which the attacker is only able to monitor the communications channel. This attack is threatens confidentiality. Examples on passive attack.[16, 18]

1. Ciphertext-only attacks: the attacker attempt to deduce the plaintext from only the ciphertext. (the attacker gets a ciphertext all of them have been encrypted using the same encryption function, and tries to find the corresponding plaintext). It have Low chance of succeeding against strong encryption. In FDSA the possibility of encrypting using the same encryption function is unpredictable, since the possibility of obtaining similar n is infeasible, while the number of bits in the encrypted data is varying with respect to n.

2. Known plaintext attacks: the attacker has access to a collection of plaintext messages and their corresponding ciphertext (the attacker has some plaintext and its matching ciphertext. The task is to find a key corresponding to this match). If same key is used to encrypt multiple blocks, frequency analysis is possible. But in FDSA its impossible to generate the same key to encrypt multiple blocks.

3. Chosen plaintext attack: the attacker gets to choose a message to be encrypted. The attacker can iteratively choose plaintext to be encrypted.

4. Chosen ciphertext attack: the attacker chooses ciphertext and sees the corresponding plaintext. (Chosen-plaintext attack, here, the attacker selects a plaintext and ciphers it using the crypt-technique he attacks. The plaintext may be chosen to ease the task of key finding). The attacker iteratively chooses ciphertext and sees the corresponding plaintext.

In each of these four attacks, the objective is to determine the key, $k \in K$, or one of its equivalent forms, that was used in encryption/decryption. In FDSA the public keys (u, v, u', v') is calculated using the system of four equations, and to find the private keys we need to solve this system with respect to five variables (x, y, x', y', n).
$u = A^n x + T_n(A)C,$
$u' = A^n x' + T_n(A)C,$
$v = B^n x + T_n(B)D,$
$v' = B^n x' + T_n(B)D$
the number of variable is more than the number of equations, so it is impossible to find a unique solution.

An active attack is one in which the attacker attempts to add, delete, or modify messages. This type of attack is threatens both confidentiality and data integrity. Examples on active attacks:

1. Man-in-the-Middle Attacks: This is a person who is able to listen to and potentially add, delete, or change messages being sent over an open

channel. This attack follows the following scenario if the sender wishes to send a message to receiver. He ask the receiver for his encryption public key, when the receiver returns key, that key is intercepted by the attacker who substitutes this key. The sender encrypts message using this bogus key and returns it. Since the attacker is the owner of this bogus key, the attacker is now able to intercept and decrypt secret messages from sender to receiver. These idea can be expressed in mathematical notation as follows:

a- Build a table of keys.

b- Compute $f(k, m)$ for every key. If f is an encryption function, m is a known message.

c- Eavesdrop a value $f(k', m)$

d- If $f(k', m) = f(k, m)$, then there is a good chance $k' = k$.

In FDSA if we receive the signature (s_1, s_2) which can be calculated using $S = (s_1, s_2) = W^n(Hm_1ux', Hm_2vy')$, then to find the corresponding plaintext, we use the following system of equations:

$$m_1 = \frac{s_1 - T_n(A)C}{(A^n x + T_n(A)C)(u' - T({}_n(A)C)}$$

$$m_2 = \frac{s_2 - T_n(B)D}{(B^n y + T_n(B)D)(v' - T_n(B)D)}$$

these two equation have three unknowns variables (n,x,y). If we try to solve this system according to the unknown variable we have an infinite number of solution.

2. A brute-force attack: is a method of breaking a cipher by exhaustively searching all possible keys. The feasibility of a brute-force attack on a cipher depends on the key space size K of the cipher and on the amount of computational power available to the attacker. As an example, imagine a system which only allows 4 digit PIN codes. This means that there are a maximum of 10,000 possible PIN trial. The difficulty of a brute force attack depends on several factors, such as: how long can the key be? how many possible values can each component of the key have? how long will it take to attempt each key? Is there a mechanism which will lock the attacker out after a number of failed attempts? However, brute force attacks against systems with sufficiently long key sizes may require billions of years to complete [4, 16].

In FDSA, the system is formalized based on function over infinite space (0,1), which is considered as open key space,then Brute-Force attack trails is infeasible, and has new problem which is the error that is attached with applying the algorithm when we want to solve nonlinear equations using numerical methods which is called "cumulative and truncation error". While the problem in other cryptosystems is the size of the key, it became here doubled, the size of the key and the type of the key.

The security of the cryptosystems that based on infinite fields functions depends on new theory from the view point of cryptography, since those cryptosystems does not depend on group structure, finite field, or discrete logarithmic equation, and most importantly, it does not depend on integer or prime numbers. Practically the classic method of attacks will fail, because they depends on solve numerically systems of nonlinear function over (0,1) to recover the unknowns, and that will involves truncation and cumulative errors. That's mean; the attractor should use the numerical methods that depend on approximation to recover the unknown variables, which will not give the exact values. There are also two important conclusions.

1. Increase the size of the key for these types of cryptosystems is not essential in increasing the security of these cryptosystems.

2. In most of the cryptosystems that depends on finite field the length of the plaintext should be less than the length of the key, while in our cryptosystem, the plain text does not have this strict condition.

5 Conclusion

In this paper, 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. The security of our protocol depends not only on the security of fractal attractor, but also on the security of Hash function and DH system. The authenticated values, (Hash function values) is a one way value.The one way property helps to ensure that the message cannot be recovered from the authenticated value easily. Known key exchange protocol like DH and RSA obtain their advantage from using

public-private key, but they are considered as secure systems via the use of very large numbers. This means that, their implementation in encryption and decryption process is slow. Therefore, using them to encrypt and decrypt a large amount of data is not preferable. We see these systems as a means of securely exchanging a symmetric key, which then are used to protect the real data we wish to exchange.

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

[1] A. Gonzalo, "Security problems with a chaos-based deniable authentication scheme," Chaos, Solitons and Fractal, 26,7-11,2005.

[2] A. Gonzalo,L. Shujun, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems",International Journal of Bifurcation and Chaos, Vol.16; No. 8, pp. 2129-2152, 2006.

[3] A. Jacquin, "Image coding based on a fractal theory of iterated contractive image transformations," IEEE Transactions on image processing, Vol.1, pp 18-30, 1992.

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

[5] A. Mohammed, A. Samsudin, A New Approach to Public-Key Cryptosystem Based on Mandelbrot and Julia, Ph.D. thesis, Universiti Sains, Malaysia. 2008.

[6] A. Mohammed,A. Samsudin, "Generalized scheme for fractal based digital signature," IJCSNS, vol.7, No. 7, July 2007.

[7] E.J.Yoon, K. Y.Yoo, "A new key agreement protocol based on chaotic maps," In proceedings of the second KES international symposium on agent and multi- agent systems: Technologies and Applications (KES-AMSTA '08), Mar., PP. 897-906, 2008.

[8] K.-H.Becker, M.DBrfler, Dynamical Systems and Fractals, Cambridge University Press, Cambridge. 1989.

[9] L.Kocarev , M. Sterjev , A. Fekete , G.Vattay , "Public-key encryption with chaos," Chaos," Dec; 14(4):1078-82,2003.

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

[11] M. Barnaey,and S. Demko, "Iterated function systems and the global construction of fractals," iroc. Roy. Sot. A 399,243-275, 1985.

[12] N. AL-Sa'idi, Md. R. Muhammad Said, "A new approach in cryptographic systems using fractal image coding," Journal of Mathematics and Statistics 5 (3): 183-189, 2009.

[13] N. AL-Sa'idi, Md. R. Muhammad Said, Fractal Attractor Based Digital Signature, in Proceedings of the 6th International Conference on Network Computing and advanced Information Management. NCM2010, Seoul, Korea, 2010

[14] P. R. Massopust, "Fractal functions and their applications," Chaos, Solitons and Fractal Vol.8, No.2, pp.171-190, 1997.

[15] P. Bergamo, P. An Od'Arco, A. De Santis, and L.Kocarev. Security of public-key cryptosystems based on Chebyshev polynomials. IEEE Transaction on Circuits and Systems, Vol.52, no.2,pp. 1382-1393,2005.

[16] S. Burton Jr.Kaliski, "An Overview of the PKCS Standards," An RSA Laboratories Technical Note, November 1, 1993.

[17] S. Kumar, "Public key cryptography system using Mandelbrot sets," Military Communications Conference, MILCOM 2006. IEEE. 23-25 Oct., 2006.

[18] S. Matsuo, K. Miyazaki, A. Otsuka, and D. Basin, "How to Evaluate the Security of Real-life Cryptographic Protocols?Financial Cryptography and Data Security,Spain, January 25-28, 2010.

[19] S. Nikiel, Iterated Function Systems for Real-Time Image Synthesis, Springer-Verlag London Limited, 2007.

[20] T.Xiang, K.Wo Wong, X.Liao, "On the security of a novel key agreement protocol based on chaotic maps," Chaos, Solitons and Fractals. 40, 672-675. 2009.

[21] W. Diffie,M.Hellman, "New directions in cryptography," IEEE Transaction on Information Theory, Vol. 22, no. 6, pp. 644-654, 1976.

[22] X. Di,X. Liao,S. Deng, "A novel key agreement protocol based on chaotic maps," Information Sciences 177,1136-1142, 2007.

Received: January, 2011