Journal of Computer Science 4 (5): 408-414, 2008
ISSN 1549-3636

Fractal (Mandelbrot and Julia) Zero-Knowledge Proof of Identity

Mohammad Ahmad Alia and Azman Bin Samsudin
School of Computer Sciences, University Sains Malaysia, 11800 Penang, Malaysia

Abstract: We proposed a new zero-knowledge proof of identity protocol based on Mandelbrot and Julia Fractal sets. The Fractal based zero-knowledge protocol was possible because of the intrinsic connection between the Mandelbrot and Julia Fractal sets. In the proposed protocol, the private key was used as an input parameter for Mandelbrot Fractal function to generate the corresponding public key. Julia Fractal function was then used to calculate the verified value based on the existing private key and the received public key. The proposed protocol was designed to be resistant against attacks. Fractal based zero-knowledge protocol was an attractive alternative to the traditional number theory zero-knowledge protocol.

Key words: Zero-knowledge, cryptography, fractal, mandelbrot fractal set and julia fractal set

INTRODUCTION

Zero-knowledge proof of identity system is a cryptographic protocol between two parties. Whereby, the first party wants to prove that he/she has the identity (secret word) to the second party, without revealing anything about his/her secret to the second party. Following are the three main properties of zero-knowledge proof of identity[1]:

Completeness: The honest prover convinces the honest verifier that the secret statement is true.

Soundness: Cheating prover can't convince the honest verifier that a statement is true (if the statement is really false).

Zero-knowledge: Cheating verifier can't get anything other than prover's public data sent from the honest prover.

In 1985, the first conceived zero-knowledge proof was given by[2]. Soon after that[3] proposed the first zero-knowledge proofs of identity. Among others there are several proposed zero-knowledge protocols such as Guillon-Quisquater proof of identity[4], zero-knowledge proofs of identity based on ElGamal[5], etc.

This study proposes a new zero-knowledge proof of identity based on Mandelbrot and Julia Fractal sets. The proposed paper is a proof method to prove and verify the true statements between two communicated parties without revealing the actual secret as described earlier.

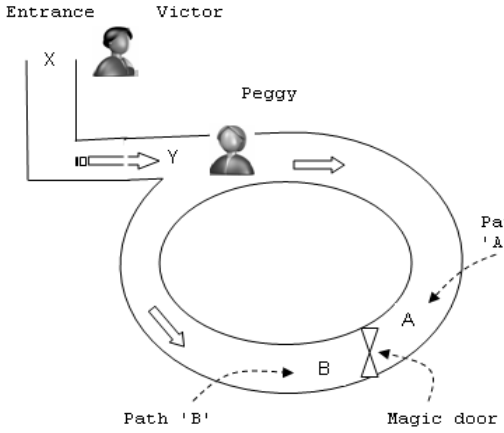


Fig. 1: Zero-knowledge cave

Zero-knowledge cave: Zero-Knowledge Cave is a well-known scenario used to describe the idea of zero-knowledge proof which was published by[6]. The scenario depicted two parties in a zero-knowledge proof protocol. The first party is known as a prover (Peggy) to prove the statement, while the second party is known as a verifier (Victor) to verify the statement.

In this story, the circle cave has one entrance and a magic door which is placed inside the cave. The scenario depicted a proof protocol between Peggy and Victor, which help Peggy to prove her knowing the secret word which will open the magic door without revealing the secret word (which can open the door) to Victor. As shown by Fig. 1 the cave paths are labeled as A for the left path and 'B' for the right path. Both Victor

Corresponding Author: Azman Bin Samsudin, School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia Tel: (604) 653 3888/ext: 2158 Fax: (604) 657 3335

and Peggy start from the cave entrance, X. First, Peggy enters the cave and randomly takes either path A or B while Victor must wait outside. Then, Victor will enter the cave to point Y and tell Peggy to appear from either path A or path B (randomly). Therefore, Peggy now can prove that she really knows the secret word by opening the magic door, if necessary and returns back to Y thru the path requested by Victor. For example, assume that Peggy knows the secret word and already she has gone inside the cave by path A and Victor ask her (randomly) to return back by path 'B', then she can open the magic door to appear on path A as requested by Victor. Assume Peggy does not know the secret word then this selection gives Peggy 50% chance of choosing properly. Repeating this protocol many times successfully makes Victor convinced that Peggy does actually know the secret word if Peggy can correctly appear all the time from the requested path specified by Victor.

Fractal: In the late 19th century, complex function has been studied by Henri Poincaré Felix Klein, Pierre Fatou and Gaston Julia in exploring Fractal. In the 1960's the study of complex plane was enhanced by the modern computer graphics, which soon gave birth to the field of Fractal geometrics[7]. Among the early work on Fractal geometric was done by Benoit Mandelbrot.

In 1960, the word Fractal was introduced by Benoit Mandelbrot 1960. The word Fractal came from a Latin word fractus meaning broken or fractured. Mandelbrot has defined the term Fractal as a fragment of geometric shape, created interactively from almost similar but smaller components[7,8]. One of the important application of Fractal involves several real applications to create realistic images of nature such as the image of clouds, snow flakes, mountains, river networks, systems of blood vessels, etc.[9,10].

Julia and Mandelbrot Fractal Sets: The Julia Fractal set (Fig. 2), developed by Gaston Julia[7], is the set of points on a complex plane and it can be created by iterating the recursive Julia function (Eq. 1). Later in 1982, Benoit Mandelbrot began his study on Julia Fractal set. He was looking for the connection between Mandelbrot set and Julia set by studying the value c from the Julia Fractal equation[11]. As the result, Mandelbrot Fractal was defined as the set of points on a complex plane by applying Eq. 2 iteratively (Fig. 2). Actually, Mandelbrot and Julia sets are both using the same basic Fractal equation as shown by Eq. 1 and 2. But the difference between them is that, Mandelbrot Fractal set iterates z^2 + c with z starting at 0, while and Julia set iterates z^2+c starting with varying non-zero z. The connection between Mandelbrot Fractal set and Julia fractal set is that, each point c in the Mandelbrot is actually specifies a geometric structure of a corresponding Julia set. That means if c is a complex point in the Mandelbrot set, there will be a Julia set connected to it. However, if c is not in the Mandelbrot set, then Julia set will become a Cantor dust[12,13]:

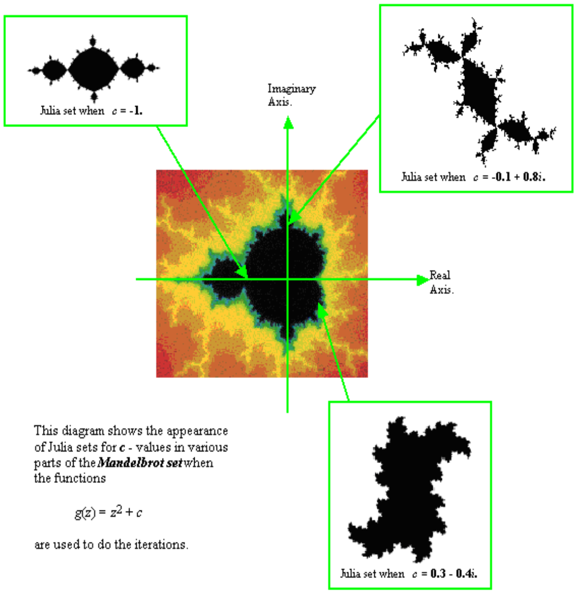

Julia set when c = -1.
Imaginary Axis.
Julia set when c = -0.1 + 0.8i.
Real Axis.
This diagram shows the appearance of Julia sets for **c** - values in various parts of the ***Mandelbrot set*** when the functions
$g(z) = z^2 + c$
are used to do the iterations.
Julia set when c = 0.3 - 0.4i.

Fig. 2: Mandelbrot and Julia Fractal image[14]

$$z_n = z_{n-1}^{\ 2} + c, c, z_i \in C, n \in Z \qquad (1)$$

$$z_n = z_{n-1}^{\ 2} + c, z_0 = 0, c, z_i \in C, n \in Z \qquad (2)$$

Mandelfn and Juliafn Function of the Mandelbrot and Julia Fractal Sets: Particularly, the Fractal can generate a specific Mandelbrot function and Julia function, Mandelfn and Juliafn respectively. Fig. 3 and 4 show images which have been generated from the Mandelfn and the Juliafn. The function f( ) in Mandelfn and Juliafn functions (Eq. 3, 4, 5 and 6) can be generate with well known functions such as sin( ), cos( ), exp( ), etc.[12,13,15]. Typically, the value which is generated by Mandelfn must belong to the Mandelbrot set and likewise, the value generated by Juliafn must belong to the Julia set[15]:

$$z_n = c \times f(z_{n-1}) \qquad (3)$$

$$f(z_{n-1}) = z_{n-1} \times c \times e,\ z_i,\ c,\ e \in C,\ n \in z \qquad (4)$$

$$z_n = c \times f(z_{n-1}),\ \ z_0 = c,\ c,\ z_i \in c,\ n \in z \qquad (5)$$

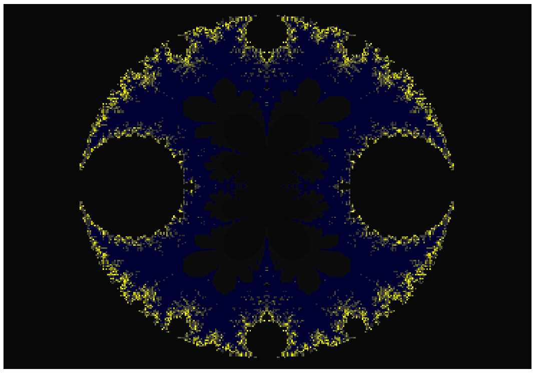


Fig. 3: Mandelfn image with the sine function (sin( ))[12]

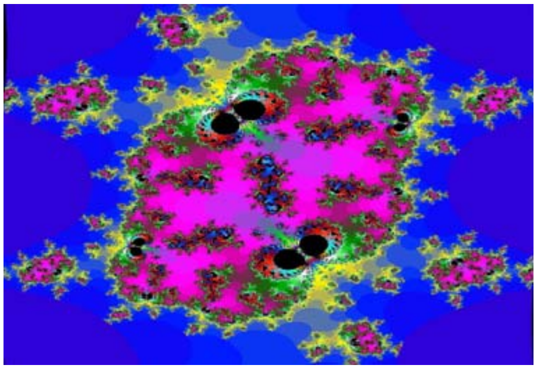


Fig. 4: Juliafn image with the cosine function (cos( ))[12]

$$z_n = c \times f(z_{n-1}),\ z_0 = y,\ \ y,\ c,\ z_i \in c,\ n \in z \qquad (6)$$

Existing proof of identity algorithm: As mentioned earlier there are a few proof of identity (PI) algorithms that had been proposed. In this Subsection we will show two well-known PI algorithms.

Feige-fiat-shamir proof of identity: Feige-Fiat-Shamir Proof of Identity protocol was the first zero-knowledge proof of identity protocol. This protocol includes two main parties, the prover (Peggy) and the verifier (Victor) in addition to the arbitrator. The working protocol is shown as follows[3,16]:

Feige-fiat-shamir proof of identity protocol:
Pre-calculation (arbitrator):

- An arbitrator generates a random modulus $n = p \times q$, where p and q are a large primes (512-1024 bits)
- The arbitrator generates a public key for Peggy, by choosing a number, v, which is a quadratic residue mod n (such that $x^2 = v \bmod n$ has a solution and $v^{-1} \bmod n$ must exist). This number, v, is the public key
- The private key is then the smallest s where $s = v^{-1} \bmod n$

The identification protocol:

- Peggy chooses a random number r where $r < n$ to compute $x = r^2 \bmod n$ and then Peggy will send x to Victor
- Victor sends Peggy a random bit, b
- If the bit is 0, Peggy sends Victor r. If the bit is 1, she sends $y = (r \times s) \bmod n$
- If the bit = 0, then Victor will verify that $x = r^2 \bmod n$, proving that Peggy knows $\sqrt{x}$
- If the bit = 1, then Victor will verify that $x = (y^2 \times v) \bmod n$, proving that Peggy knows $\sqrt{\frac{x}{v}}$

Guillou-quisquater proof of identity: This protocol has been used in smart card applications, as it uses the minimum size of accreditation (i.e., each round). The prover in this protocol must choose the following[4,16]:

- A credentials J (card ID, validity, bank account number, etc.) as a public key
- An exponent v
- A modulus n, which is the product of two large secret primes
- The private key B is calculated so that $JB^v = 1 \bmod n$

Guillou-Quisquater Proof of Identity protocol:

- Peggy has to prove her credentials to Victor. Therefore, Peggy sends Victor her credentials J
- Peggy chooses a random number r, such that $1<r<n-1$
- Peggy computes $T = r^v \bmod n$ and then sends T to Victor
- Victor chooses a random number d, such that $0<d<v-1$ and then he will send d to Peggy
- Peggy computes $D = rB^d \bmod n$ and sends D to Victor
- Victor computes $\check{T} = (D^v \times J^d) \bmod n$. If $T = \check{T} \bmod n$, then the authentication succeeds

MTERIAL AND METHODS

Fractal (Mandelbrot and Julia Sets) zero-knowledge proof of identity: This research describes the proposed zero-knowledge proof of identity based on Mandelbrot and Julia Fractal sets protocol in detail. The proposed

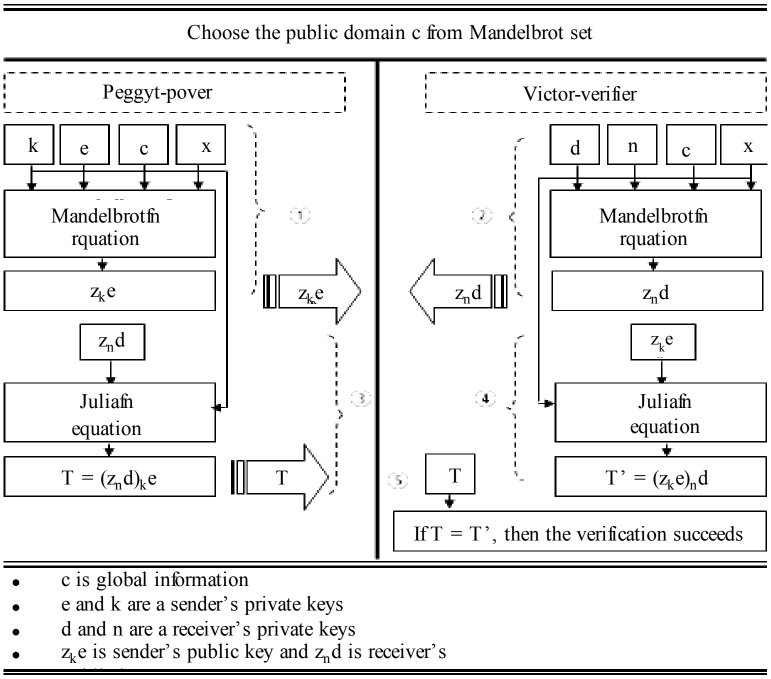


Fig. 5: Fractal zero-knowledge protocol

zero-knowledge communication protocol involves two parties, the prover as Peggy and the verifier as Victor. The first step in this protocol is to generate the public key and the private key by using Mandelbrot and Julia functions. In the proposed protocol we use the Mandelbrot function, Mandelfn and Julia function, Juliafn as shown by Eq. 4 and 5.

As we have shown in Fig. 5, Fractal zero-knowledge protocol involves two parties, Peggy and Victor. Peggy tries to prove her identity (secret keys (k and e)) to Victor without telling the secret itself (Eq. 7). Therefore, Peggy must generate the public key ($z_k e$,) based on her private key by using Mandelfn and then sends it to Victor (Fig. 5, Step 1). Victor on the other hand will do the same and send his public key ($z_n d$) to Peggy (Fig. 5, Step 2). The generated public key, $z_n d$, is calculated by using Mandelfn equation as shown by Eq. 8:

$$z_k e = z_{k-1} \times c^2 \times e,\ z_i,\ c,\ e \in c,\ k \in z \quad (7)$$

$$z_n d\ = z_{n-1} \times c^2 \times d, z_i,\ c,\ d \in c,\ n \in z \quad (8)$$

After exchanging the public keys between Peggy and Victor, Peggy will execute the Juliafn function with her secret keys to compute T (Fig. 5, Step 3) and then she will send T to Victor. Victor then will try to verify Peggy's secret by computing T' (Fig. 5, Step 4). If T = T', then Victor can verify that Peggy knows the secret and then the authentication is succeeded (Eq. 9):

$$\begin{gathered} T = c^{k-x} \times (z_n d)\ _k e, \\ T' = c^{n-x} \times (z_k e)\ _n d, \\ z, c, e, d \in c, n, x, k \in z \end{gathered} \quad (9)$$

Working Example of The Proposed Protocol: This example was coded in C by using GMP to simulate the 64-bit complex numbers. In this example each complex number is being represented by a 64-bit value. Table 1 shows a working example of the proposed protocol. In this example, the global information, c, is initialized to a complex value (-0.1155056) + (-0.359816)i and x is initialized to 3 (The value of x is used to reduce the final calculation (Eq. 9) and can be set to 0, if desired). At the beginning, Peggy and Victor need to choose their private keys (Table 1, row 1). Then they have to calculate the corresponding public keys as shown by Table 1, Row 2, by using the Mandelbrot function, Mandelfn. These values are $z_k e$ (Peggy's public key) and $z_n d$ (Victor's public key). Table 1, Row 3, shows both parties exchanging their public keys. Following this process is the calculation of the verified value by using Julia function, Juliafn. Peggy will produce the value, $(z_n d)_k e$, after executes the

Table 1: Example of fractal zero-knowledge protocol

Description	Peggy	Victor
Random integer numbers	k = 7, e = 0.50001002-0.50001002	n = 6, d = 0.84000007-0.84000007
(Private values)		
Compute by Mendelfn formula	z_ke = 0.00000195711318546643848258	z_nd = 0.00125328392603999767482
(Public values)	+0.000000568900570672474295198	-0.0095657700955645971744
Peggy sends z_ke. Victor sends z_nd	0.00125328392603999767482	0.00000195711318546643848258
	-0.0095657700955645971744	+0.000000568900570672474295198
Compute by Juliafn formula:		
Ť’ = $(z_k e)_n$d	T = 0.000166578803014891038796	Ť‘ = 0.000166578803014891038796
T = $(z_n d)_k$e	+0.0000180504674723535012322	+0.0000180504674723535012322.
T = Ť‘?	0.000166578803014891038796	0.000166578803014891038796
	+0.0000180504674723535012322	+0.0000180504674723535012322.

Juliafn with (k, e) (Peggy’s private key). Similarly Victor will verify the secret by executing the Juliafn function with (k, d) (Victor’s private keys) and z_ke (Peggy’s public key) as the input parameters to compute the value z_ke. This process is shown by Row 4 of Table 1. In Row 5 of Table 1, Victor can verify that the values of T and Ť are indeed the same.

RESULTS AND DISCUSSION

Security analysis of the proposed protocol: Fractal Cryptography is based on a NP-hard problem[12,13,17]. Therefore, the attack on the proposed zero-knowledge proof of identity protocol is computationally impossible because of the iteration parameter k (or n) and the variation constant e (or d), which are unknown to the public. Also, this will prevent attacks on the private values, given that d and e are represented appropriately. We suggest that the value of d and e be represented by a 128-bit value which should give 2^{128} possibilities for every value of n (or k) that are being attacked with a brute force attack[12].

Statistical analysis: Statistical analysis helps to demonstrate the strength of cryptography algorithms[18]. It is well known that many zero-knowledge proof of identity protocols have been successfully proved and analyzed by using statistical analysis. Therefore, an ideal zero-knowledge proof of identity should be resistant to the brute force of any statistical attack. Statistical analysis has been performed to prove the strength of the proposed zero-knowledge proof of identity based on Mandelbrot and Julia Fractal sets by calculating the correlations coefficient analysis of two adjacent points.

Correlation test for the proposed zero-knowledge proof of identity: The correlation test is a statistical analysis tool. It is used to find the correlation value between two distributed points. In this Subsection, the correlation between two adjacent points has been used to perform the statistical analysis on the proposed Fractal zero-knowledge proof of identity. Correlation coefficient was calculated by using Eq. 10, 11, 12, 13 and 14:

$$\mathrm{cov}(x, y) = E(x - E(x)(y - E(y)) \tag{10}$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{11}$$

where, x and y are the values of two adjacent points. In numerical computations, the following discrete formulas have been used:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{12}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{13}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{14}$$

This Subsection presents the correlation values for several tests on the verified key values. The verified secret values have been calculated by using general numbers for the global value and the receiver’s private keys. We have calculated 256 correlation pairs by using Eq. 11 to find the correlation average. The correlation tests are based on the changing of the sender’s private keys value 128 times on the key, e, as well as 128 times on the private key, n (Fig. 6a). Also, Fig. 6b shows the absolute values of the correlation tests. As shown by Fig. 7, we have designed the correlation coefficient tests by changing only one bit at a time for the key value and compared them with a predetermine control value. The key e is initialized to 1 (000…001) and then the bit 1 is moved one bit at a time to the left. All the

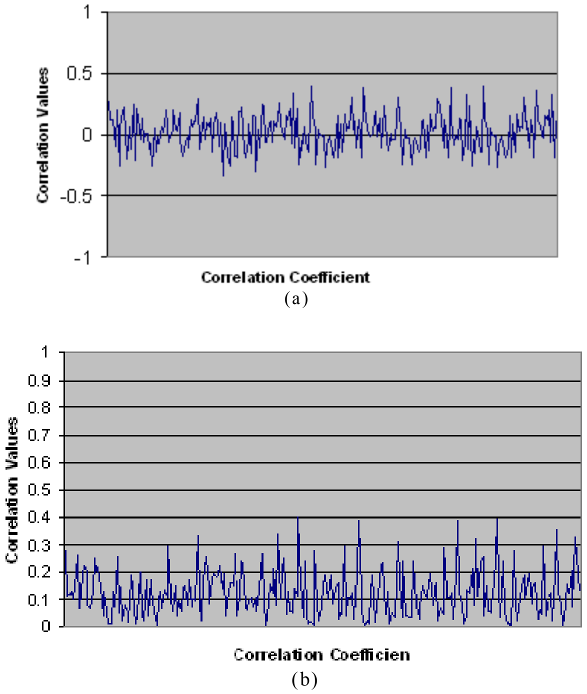
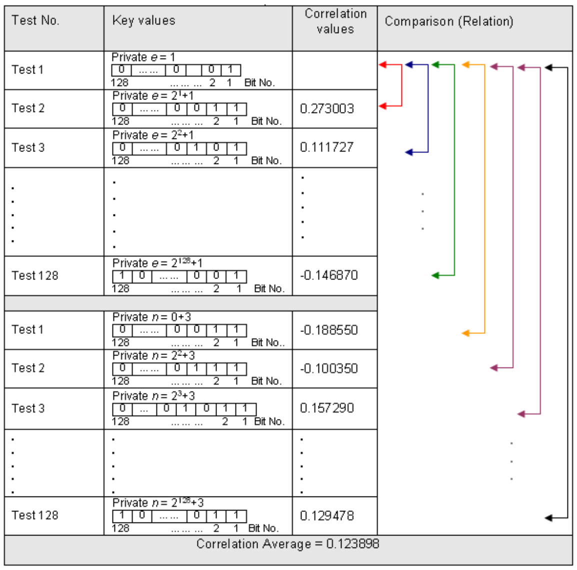


Fig. 6: (a): Correlation results for the proposed zero-knowledge proof of identity protocol (b): The absolute values of the correlation results for the proposed zero-knowledge proof of identity protocol

Table 2: Typical interpretation of the correlation coefficient (r)[19]

Correlation range	Interpretation of "r"
±(0-0.20)	No correlation
±(0.20-0.40)	Low degree of correlation
±(0.40-0.60)	Moderate degree of correlation
±(0.60-0.80)	Marked degree of correlation
±(0.80-1.0)	High correlation

generated values of e's will then compared with the control value of 000…001. For the private value n, we have initialized n to 3 (rather than 1) which make the iterations more efficient on the first correlation test and then the value of n is also changed one bit at a time as explained earlier. The absolute value for the average correlation results between two adjacent points for the verified secret key values is 0.123898 (Fig. 3). Since the correlation average is very close to zero and between 0 and 0.20, we can conclude[19] that there is no correlation between the distributed points for the verified secret key value (Table 2). The uncorrelated result highlights the difficulty to attack the secret key by analyzing the correlation between verified secret keys.



Test No.	Key values	Correlation values	Comparison (Relation)
Test 1	Private $e = 1$ 0 | ...... | 0 | | 0 | 1 128 .... 2 1 Bit No.		
Test 2	Private $e = 2^1+1$ 0 | ...... | 0 | 0 | 1 | 1 128 .... 2 1 Bit No.	0.273003	
Test 3	Private $e = 2^2+1$ 0 | ...... | 0 | 1 | 0 | 1 128 .... 2 1 Bit No.	0.111727	
. . . . .	. . . . .	. . . . .	
Test 128	Private $e = 2^{128}+1$ 1 | 0 | ...... | 0 | 0 | 1 128 .... 2 1 Bit No.	-0.146870	
Test 1	Private $n = 0+3$ 0 | ...... | 0 | 0 | 1 | 1 128 .... 2 1 Bit No..	-0.188550	
Test 2	Private $n = 2^2+3$ 0 | ...... | 0 | 1 | 1 | 1 128 .... 2 1 Bit No.	-0.100350	
Test 3	Private $n = 2^3+3$ 0 | ... | 0 | 1 | 0 | 1 | 1 128 .... 2 1 Bit No.	0.157290	
. . . . .	. . . . .	. . . . .	
Test 128	Private $n = 2^{128}+3$ 1 | 0 | ...... | 0 | 1 | 1 128 .... 2 1 Bit No.	0.129478	
Correlation Average = 0.123898			

Fig. 7: Correlation coefficient for the proposed zero-knowledge proof of identity protocol

CONCLUSION

This research has shown the possibility of using Fractal sets (Mandelbrot and Julia Fractal sets) in cryptographic zero-knowledge protocol. The Fractal based zero-knowledge protocol is made possible because of the intrinsic connection between the Mandelbrot and Julia Fractal sets. The security of the proposed Fractal zero-knowledge protocol depends on the number of iterations which convert the initial value c in the Mandelbrot Fractal equation to the starting value of z for Julia Fractal equation. Adding the key e during the iteration of Mandelbrot and Julia functions introduces the needed complexity of the proposed protocol. Furthermore, we can identify that the security of the proposed Fractal zero-knowledge proof of identity is based on the chaos NP-hard problem and the randomness of the output generated as shown by the correlation test.

ACKNOWLEDGMENT

The authors would like to thank the Universiti Sains Malaysia (USM) for supporting this study.

REFERENCES

1. Adelsbach, A. and A. Sadeghi, 2001. Zero-knowledge watermark detection and proof of ownership. In: Information Hiding: Fourth International Workshop, Springer-Verlag, Berlin Germany, LNCS 2137, April 25 - 27, 2001, pp: 273-288.

2. Goldwasser, S., S. Micaliand C. Rackoff, 1985. The knowledge complexity of interactive proof systems. In: ACM Symposium on Theory of Computing, ACM Press, New York, USA, May 06 - 08, 1985, pp: 291-304. DOI= http://doi.acm.org/10.1145/22145.22178.
3. Feige, U., A. Fiat and A. Shamir, 1987. Zero knowledge proofs of identity. In: Annual ACM Symposium on Theory of Computing, ACM Press, New York, USA, A. V. Aho, Ed. STOC '87, May-1987, pp: 210-21. DOI= http://doi.acm.org/10.1145/28395.28419.
4. Guillou, L. and J. Quisquater, 1988. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. In: Proceeding, Lecture Notes in Computer Science on Advances in Cryptology-EUROCRYPT'88, Springer-Verlag, New York, May 25-27, 1988, pp: 123-128.
5. Zhang, D., M. Liu and Z. Yang, 2004. Zero-knowledge proofs of identity based on elgamal on conic*. In: Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04), Washington, DC, USA, Sep 13-15 2004, pp: 216-223. DOI= http://doi.ieeecomputersociety.org/10.1109/CEC-EAST.2004.77.
6. T. Berson, 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.
7. Benoît, B. and Mandelbrot, 1982. Fractal Geometry of Nature. W.H. Freeman, San Francisco, First Edition, pp: 4-20, 30-70. ISBN:0716711869, 9780716711865.
8. Peitgen,:0-387-97041-X.
9. Patrzalek, E., 2006. H.O., H. Jrgens and D. Saupe, 1992. Fractals for The Classroom-Part One: Introduction to Fractals and Chaos. First edition, Springer-Verlag New York, Inc. ISBN Fractals: Useful Beauty (General Introduction to Fractal Geometry). Stan Ackermans Institute, IPO Centre for User-System Interaction, Eindhoven University of Technology, pp: 1-7. DOI= http://www.fractal.org/Bewustzijns-Besturings-Model/Fractals-Useful-Beauty.htm
10. Kaoru, K. and W. Ogata, 1999. Efficient rabin-type digital signature scheme, Springer, Number theory and combinatorics, Designs, codes and cryptography, 16: 53-64. DOI = 10.1023/A:1008374325369
11. Lazareck, L., G. Verch and J.F. Peter, 2001. Fractals in circuits. IEEE Conf., 1: 589-594.
12. Alia, M. and A. Samsudin, 2007. A new digital signature scheme based on mandelbrot and julia fractal sets. Am. J. Applied Sci., 4: 850-858.
13. Alia, M. and A. Samsudin, 2007. A new public-key cryptosystem based on mandelbrot and julia fractal sets. Asian J. Inform. Technol., 6: 567-575.
14. Alia, M. and A. Samsudin, 2008. Survey on Fractal (Mandelbrot and Julia Sets) Public-Key Cryptosystem. National Conference on Information Retrieval and Knowledge Managment (CAMP08), March 18-19 2008. DOI= http://www.upnm.edu.my/CAMP08/brochureCAMP08.pdf
15. Noel and Giffin, 2006. Fractint. In: TRIUMF project. The University of British Columbia Campus in Vancouver B.C. Canada, pp : 1-7.
16. Hannu, A., 1995. Zero Knowledge Protocols And Small Systems. In: Network Security Seminar (Tik-110.501), Helsinki University of Technology, Finland, Nov. 2-4 1995, pp: 1-15.
17. Ruhl, M. and H. Hartenstein, 1997. Optimal Fractal Coding Is NP-Hard. In: Proceedings of the 7th Data Compression Conference, DCC97, March 25-27 1997, Snowbird, Utah, pp: 261-270.
18. Behnia, S., A. Akhshani, A. Akhavan and H. Mahmodi, 2007. Applications of Tripled Chaotic Maps in Cryptography, arXiv.org, The Cornell University Library. DOI= http://arxiv.org/abs/0705.2633v1.
19. Abraham, N. and Franzblau, 1958. A Primer of Statistics for Non-Statisticians. 4th Edn,. Harcourt, Brace, New York.