Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Analytical Approach to Encryption using Superior Mandelbrot and Superior Julia Sets

Abhishek Shukla *
I.T.Department&RDEC,GZB
India.

Vijay Singh
CSE Department&SRMCEM, LKO
India.

Mithlesh Kr. Mishra
MCADepartment&RDEC,GZB
India.

Chandramani Srivastava
CSE Department&RDEC,GZB
India.

Abstract— The voluminous digital data exchange between various computers has introduced large amount of security vulnerabilities. Encryption schemes have been increasingly studied to meet the demand for real-time secure transmission of data over the Internet and through wireless networks. In this paper, we try to study a new cryptographic key exchange protocol based on superior Mandelbrot and Superior Julia sets. In this study we analyze a cryptographic system utilizing fractal theories; this approach uses concept of public key cryptography by taking advantage of the connection of Superior Julia and Superior Mandelbrot sets. This paper exploits the main feature of public key security.

Keywords— Superior Mandelbrot and Julia sets, Fractal geometry, Public keysecurity

I. INTRODUCTION

Enhanced security will deinitely be a great relief for paranoid people. RSA cipher is most commonly used for public-key encryption depends on the dificulty of factoring large numbers (Stallings., 2003) [27]. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key (Rivest et al., 1978) [24].

This study proposes a new fractal (based on Superior Mandelbrot and Superior Julia sets) encryption key protocol which secures transmission of data between computers. The working of the proposed scheme depends on the strong interconnection between two Superior Julia and Superior Mandelbrot sets which generates the corresponding public and private keys. Cryptography is classiied into Symmetric key(Secret Key) cryptography (ig. 1) and Asymmetric key (Public key) cryptography [27]. In Modern PKC algorithms, there is a pair of keys, one of which is known to the public and used to encrypt the plaintext to be sent to the receiver who owns the corresponding decryption key, known as the private key (fig. 2). In general, a security protocol uses public-key cryptosystem to exchange the secret key between communicating nodes and then uses secret-key algorithms with the agreed secret key as the password to ensure conidentiality on the data transferred (Branovic et al., 2003; Menezes et al., 1996) [2].

Fig. 1: Symmetric Key Cryptography

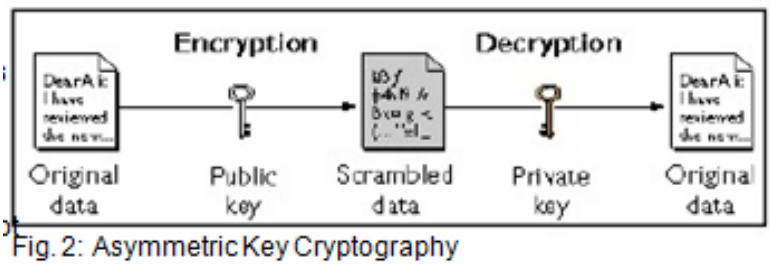
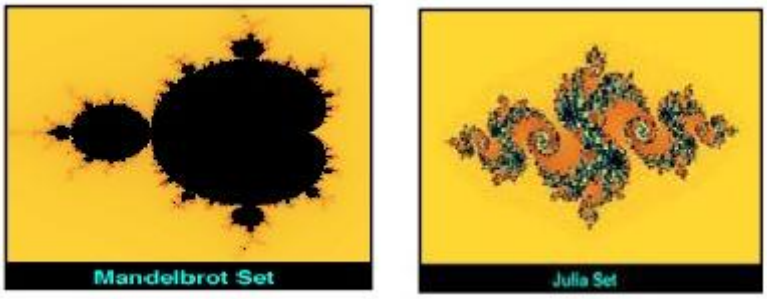


Fig. 2: Asymmetric Key Cryptography

Fractal is a geometric pattern that cannot be represented by classical geometry as it is a geometric igure that repeats itself under several levels of magniication; a shape that appears irregular at all scales of length, e.g. a fern. This geometric ig., built up from a simple shape, by generating the same or similar changes on successively smaller scales; it shows self-similarity. This means they usually contain little copies of themselves buried deep within the original and also have ininite details. The repetition of form over a variety of scales is called self similarities. The bigger eddies in a turbulent low look much the same as the smaller ones, and vice versa.

Fractals are used especially in computer modeling of irregular patterns and structures in nature. The backbone of the fractal is iteration method i.e. feedback system. In other words the same process is performed repeatedly i.e.the output of the system acts as an input for next one. 'Fractal' has its origination from a Latin word 'fractus', which means 'to break'. The term fractal was first coined by B. B. Mandelbrot in 1975, which is also known as the 'father of fractal geometry'. Fractal are usually characterized as having non-integer dimensions and are an example of a Chaos system, where by changing the initial parameters to the system, even slightly, can generate a totally new Fractal image altogether [7].



(a) (b)

Fig. 3:The Mandelbrot Fractal set (see ig. 3) is the set of points on a complex plane. The Fractal image can be generated by applying Equation 1 recursively [13].

$$Z_n = Z_{n-1}{}^2 + c; Z0 = 0; c, Z_n \in c; n \in Z \qquad (1)$$

$$Z_n = Z_{n-1}{}^2 + c; Z0 = 0; c, Z_{n-1} \in c; n \in Z \qquad (2)$$

The difference between the Mandelbrot set and the Julia set is that the Mandelbrot set iterates $Z_{n-1}{}^2 + c$ with Z starting at 0 and varying c with every iteration, while Julia set iterates $Z_{n-1}{}^2 + c$ for fixed c and starting with non-zero value of Z [6, 10]. All points, Z_n ,must reside on the Mandelbrot set or the Julia set, respectively. In our work, we are depending on the intrinsic connection between both of the Mandelbrot and the Julia Fractal sets. The connection between the Mandelbrot set and the Julia set is that each point c in the Mandelbrot set specifies the geometric structure of the corresponding Julia set.

II. REVIEW OF LITERATURE

Recently Rani and Kumar [18] have given the concept of Superior Julia set and Superior Mandelbrot set [17-18] in the study of discrete dynamical system. They can be used effectively to play a significant role in cryptographic security. Further with the help of complex variables efficient algorithms can be generated.

A. Superior Mandelbrot and Superior Julia Sets

(Rani and Kumar [18]). The superior Mandelbrot set (SM set) for the polynomial $Q_{m,c}(z) = z_m + c, \; where \; m>1$ is a positive integer, is defined as the collection of values of c for which the superior orbit of $z = 0$ does not escape to infinity. Ihe Mandelbrot sets for $Q_{m,c}(z)$ are SM sets with $\beta = 1$. The escape criterion plays a vital role in the generation and analysis of Mandelbrot sets and its variants. This paper extends their following result, which gives a general escape criterion for the polynomial $Q_{m,c}(z), m>2$. The Superior Julia sets is the set of points whose orbit are bounded under the superior iteration of the function $Q_{m,c}(z)$, where $\{\beta_n\}$ converges to a non-zero number between $0 \; \& \; 1$. The general superior escape criterion for the function $Q_{m,c}(z) = z_m + c$ is given by max $\left\{|c|, (2/\beta_n)^{1/m-1}\right\}$ where, $0 < \beta_n <= 1, n = 1, 2, ...m > 1$ & a positive integer and c is a complex parameter.

B. Public Key Encryption based on the Superior

Mandelbrot and Superior Julia Sets Most of the currently used public-key primitives are computationally expensive with relatively lengthy key requirement due to dependency on the number theory, which the primitives were derived from. Therefore, it's important to develop (investigate) new cryptography primitives from other mathematical hard problem (NP hard) which is directly not based on number theory. In this work, we propose new public-key primitives based on Superior Mandelbrot and Superior Julia Fractal sets. However, this study attempts to deal with the following problems which are related to Cryptographer requirements:

1. Key size and variation: most of public-key Cryptography protocols depend on a large prime key that to ensure the security of these protocols and prevent a brute force attack.
2. Algorithm speed: a lot of the public-key Cryptography protocols perform at a low speed depending on key size.
3. Performance evaluation: some of the public-key protocols provide high level of security at a much higher cost.

These arguments lead to other problems which are related to the security in the user's applications through the open network. These problems are represented by the wide internet access and its applications such as e-payment, e-business, etc. The problems of attacks which are faced by cryptanalysts have made us look for the new system that can be applied to the cryptosystem. Our study in this thesis focuses on the Fractal which is a NP-hard problem (hard to cryptanalyst).This study proposes new public-key primitives based on Superior Mandelbrot and Superior Julia Fractal sets. The creation of the Fractal based public-key primitives is possible because of the strong connection between the Mandelbrot and Julia Fractal sets[28]. Since fractal Sets are based on complex number theory and Fractal images can be represented with some complex variable. It gives rise to the fact that Cryptosystem can be further enhanced by using encryption through Fractal images. In the proposed protocols, Mandelbrot Fractal function takes the chosen private key as the input parameter and generates the corresponding public key. Julia Fractal function is then used in accordance with the function and the required algorithm specifically. In the key exchange protocol, the Julia function is used to calculate the shared key based on the existing private key and the received public key. In the public-key encryption algorithm, the Julia function is used to encrypt the plaintext with the receiver's public key and decrypt the cipher text based on the receiver's private key. Finally, in the digital signature scheme, the Julia function is used to sign the message with the receiver's public key and verify the received message based on the receiver's private key. In addition, another variation of the signature algorithm is proposed where the verification can be made by the general public. In this alternative method, the sender will generate his public and private keys by Mandelbrot function and then the Julia function will be used by the public to verify the message based on the sender's public keys. The proposed public-key [7] primitives were designed to be resistant against attacks, utilize small key size and perform comparatively faster than most of the existing public-key primitives such as RSA (Rivets, Shamir and Adleman), DH (Diffie Hellman) [24] etc. The proposed Fractal public-key primitives are, therefore, an attractive alternative to the traditional number theory based public-key primitives.

III. Superior Mandelbrot and Superior Julia Sets Used for Key Generation in RSA

In the proposed protocol sender and receiver will agree and use a public domain value, c. The receiver and sender generates their private key in the form of (e,n) and (k,d) respectively. As these keys are generated both sender and receiver will use their private key values and the value of c as input to the superior Mandelbrot function to produce the public keys $z_n d$ and $z_k e$. And then both sender and receiver must exchange the public keys. Using key distribution authorities sender will obtain receiver's public key, $z_n d$ and uses this value together with her private key and the plaintext, as inputs to the Superior Julia sets to produce cipher text V which will be sent to Bob. To retrieve the original text receiver must have sender's public key, $z_k e$ and the cipher text V which will then be used as input values together with his own private key to Superior Julian function for deciphering V.

Fig. 4 proposes use of the Superior Mandelbrot and Superior Julia sets For public and private key generation

IV. Conclusion

The problems of attacks which are faced by cryptanalysts have made us look for the new system that can be applied to the cryptosystem. Our study in this thesis focuses on the Fractal which is a NP-hard problem (hard to cryptanalyst).This study proposes new public-key primitives based on Superior Mandelbrot and Superior Julia Fractal sets. The creation of the Fractal based public-key primitives is possible because of the strong connection between the Mandelbrot and Julia Fractal sets [28]. Further by using different iterative procedures and more fractal concepts we can make more efficient and increased performance algorithm for the same.

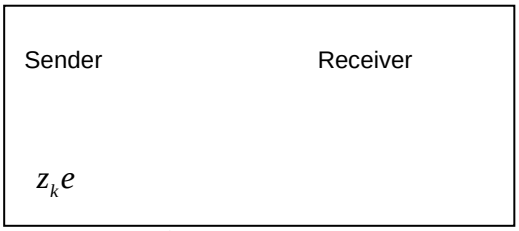


Fig. 4:

REFERENCES

[1] Atul Khate,"Cryptographic and Network Security", TMH, 2007.

[2] A. Menzes, P. Van Oorschot, S. Vanstone,"Handbook of Applied Cryptography", CRC Press, 1996, pp. 425–488.

[3] A. MS,"Public Key Cryptography: Applications Algorithms and Mathematical Explanations," India, Tata Elxsi, 2007.

[4] B. Preneel, P. van Oorschot,"On the security of two MAC algorithms", Advances in Cryptology { Eurocrypt 96 Proceedings, Lecture Notes in Computer Science} Vol. 22, U. Maurer ed., Springer-Verlag, 1996.

[5] B. Preneel, K. Mercierlaan,"Cryptanalysis of Message Authentication Codes", Department Electrical Engineering, Katholieke Universiteit Leuven, Belgium, 2004.

[6] C. Hsu, Y. Hou,"Visual cryptography and statistics based method for ownership identiication of digital images", in Proc. of the International Conference on Signal Processing (ICSP'2004), Istanbul, Turkey, 2004, pp. 221–224.

[7] D.G. Piche,"Complex bases, number systems and their application to fractal-wavelet image coding", Ph.D. Thesis in applied Mathematics. Waterloo, Ontario, Canada, 2002.

[8] Damgard,"A design principle for hash functions", Advances in Cryptology { Crypto 89 Proceedings, Lecture Notes in Computer Science Vol. 435, G. Brassard ed., Springer-Verlag, 1989.

[9] F. Yang,"Cryptanalysis on an Algorithm for Eficient Digital Signatures", Cryptology ePrint Archive 2005/456, 2005.

[10] H. Dobbertin,"The Status of MD5 After a Recent Attack", RSA Labs' CryptoBytes, Vol. 2 No. 2, Summer 1996.

[11] H. El-Bolok, T. A. El-Mageed, N. A. El-Salam, I. A. Elgtawal, "Public Key Cryptosystems and its Applications in Digital Signature", Helwan University, Faculty of Engineering, 2003.

[12] J. L. Dugelay, E. Polidori, S. Roche (1996),"Iterated Function Systems for still Image Processing", IWISP-96, Manchester, UK, 2005.

[13] M. Barnsley,"Fractals Everywhere", 2nd Edn., Academic Press Professional Inc., San Diego, CA, USA., pp. 550,1993.

[14] M. Barnsley, S. Demko, (1985),"Iterated function systems and the global construction of fractals", Proc. R. Soc. London, 399, pp. 243-275. [Online] Available: http://adsabs.harvard. edu/abs/1985RSPSA.399.243B

[15] M. Bellare, R. Guferin, P. Rogaway, "XOR MACs: New methods for message authentication using nite pseudorandom functions", Advances in Cryptology { Crypto 95 Proceedings, Lecture Notes in Computer Science Vol. 963, D. Coppersmith ed., Springer-Verlag, 1995.

[16] M. Mogollon,"Cryptography and Security Services: Mechanisms and Applications," University of Dallas, USA, 2007.

[17] Mamta Rani,"Iterative procedures in Fractals and Chaos", Ph.D. Thesis, Department of computer Science, Faculty of technology, Gurukula Kangri Vishvavidyalaya, Hardwar, 2002.

[18] M.Rani, V. Kumar, "Superior Mandelbrot set", J. Koreans Soc. Math. Edu. Ser. D (2004) 8 (4), pp. 279-291.

[19] Neal Koblitz, "ACourse in Number Theory and Cryptography",2rd Edn., Springer, pp. 235, 1994.

[20] "National Institute for Standards and Technology", Digital Signature Standard (DSS)", Federal Register, Vol. 56, No. 169, 1991.

[21] O. Goldreich, S. Goldwasser, S. Micali, "How to construct random functions", Journal of the ACM, Vol. 33, No. 4, pp. 210-217, (1986).

[22] R. Atkinson,"Security Architecture for the Internet Protocol", IETF Network Working Group, RFC 1825, 1995.

[23] R. Atkinson, "IP Authentication Header", IETF Network Working Group, RFC 1826, 1995.

[24] R. Rivest, A. Shamir, L. Adleman,"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol. 21, No. 2, pp. 120–126, 1978.

[25] T. ElGamal,"A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Trans. Inform. Theory IT, Vol. 31, no. 4, pp. 469–472, 1985.

[26] W. Difie, M. Hellman, "New Directions in Cryptography", IEEE Transactions in Information Theory, Vol. It 22, No. 6, 1976.

[27] William Stalling,"Cryptography And Network Security", PHI, 2004.

[28] Y. C. Hou, S. F. Tu,"A Visual Cryptographic Technique for Chromatic Images Using Multi-pixel Encoding Method", Journal of Research and Practice in Information Technology, Vol. 37, No.2, pp. 179-192, 2005.

[29] Y. Fisher,"Fractal Image Compression", Theory and Application, Springer-Verlag, New York, USA, pp. 341, 1995.

