Finite and Infinite Field Cryptography
Analysis and Applications

Nadia M. G. AL-Saidi, Mohamad Rushdan Md. Said, and Arkan J. Mohammed

Abstract—Most of the currently used cryptosystems are defined over finite fields and use modular arithmetic. Their security is often based on the difficulty of solving certain number theoretic problems. In recent years, a large amount of work for introducing of systems defined on infinite field in the design of new cryptosystems has been published. Many studies have been done by introducing of chaotic and fractal functions into the design of symmetric and asymmetric encryption scheme. This paper aims to discuss the advantages and drawbacks of using these new types of mathematics methods behind computer and network security that emerge as a result of integrating between communication and information sciences. In this paper the analysis and the comparison studies between these two disciplines is discussed in terms of their efficiency and security, to identify a common framework for the guidelines that address main issues for implementation and security analysis. Conclusions on their performance are inferred.

Keywords—Fractal, Chaos, Private Key, Public Key.

I. INTRODUCTION

Cryptography is the study of mathematical and computational techniques related to aspects of information security. It is a method of transferring private information and data through open network communication [1]. With the rapid development in the information science, there is a growing demand of cryptographic techniques, which has spurred a great deal of intensive research activities in the study of cryptography. The difficulty of solving some theoretic problems such as factorization and discrete logarithm in finite multiplicative groups, controlling the security of these techniques.

Current cryptographic techniques are based on number theoretic or algebraic concepts. Chaos and fractal are another paradigm, which seems promising. They are an offshoot from the field of nonlinear dynamics and have been widely studied. Their behavior is a apparently looks random. The use of fractal and chaos have advantage since; only few parameter would have to be stored, and this kind of key is very robust to attacks for two reasons; first, 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 an infinite space [2].

This paper aims to discuss the advantages and drawbacks of using these new types of mathematics methods behind computer and network security that emerge as a result of integrating between communication and information sciences in recent years from three different aspects: first, the development of new encryption techniques that ensures high security, complexity, easy to implement, etc.; second discuss the challenges of mathematics needed in cryptanalysis aspect and finally anew methods of evaluation used to evaluate the security of modern systems by using new mathematical methods [3].

The outline of this study is organized as follows; In Section II some material and methods about finite and infinite fields are described briefly, comparison studies between cryptosystem based on these sets is accomplished. The main respective advantage and disadvantage are point out also. Section III is devoted to discuss the two systems in terms of their performance and security analysis,. The conclusion are drawn in Section IV.

II. MATERIAL AND METHODS

A. Finite field Cryptosystems

It is almost impossible to fully understand practically any facet of modern cryptography and several important aspects of general computer security if you do not know what is meant by a finite field. For example, without understanding the notion of a finite field, you will not be able to understand AES (Advanced Encryption Standard), which is supposed to be a modern replacement for DES. The substitution step in AES is based on the concept of a multiplicative inverse in a finite field. Also without understanding finite fields, you will NOT be able to understand the derivation of the RSA algorithm for public-key cryptography, and if you do not understand the basics of public-key cryptography, you will not be able to understand the workings of several modern protocols that used for secure communications over networks. You will also not be able to understand modern security concepts such as

---

Nadia M.G. Al-Saidi is with Applied Sciences Department-Applied Mathematics University of Technology -Baghdad-Iraq, Tel : +9647901305365/ e-mail: nadiamg08@gmail.com
Mohamad Rushdan Md. Said is with Institute for Mathematical Research Putra Malaysia Serdang, Malaysia e-mail nrushdan@fsas.upm.edu.my
Arkan J. Mohammed is with the Department of Mathematics-College of Science-Al-Mustansiriah University e-mail: drarkanjasim@yahoo.com.
authenticity and digital signature.

Another example about the important of a finite fields that you will never understand the up and coming Elliptic Curve Cryptography (ECC) algorithm that which consider to be a replacement for RSA for public key cryptography.

A finite field is defined to be a set of numbers in which you can carry out the operations of addition, subtraction, multiplication, and division without error. In ordinary computing, division particularly is error prone and what you see is a high precision approximation to the true result. Such high-precision approximations do not suffice for cryptography work. All arithmetic operations must work without error for cryptography.

The basic concepts related to any cryptosystem designed on a finite fields, are: plaintext $P$, Ciphertext $C$, Keyspace $K$, in addition to the encryption rule $e_{s}$, and decryption rule $d_{s}$, where $e_{s}: P \rightarrow C$, and $d_{s}: C \rightarrow P$, that satisfied $d_{s}(e_{s}(x))=x$. The Cryptosystem is a five-tuple $(P,C,K,e_{s},d_{s})$ defined on a finite set. All the sets $M,P,C$ are known, only the pair $(K^{*},K^{n})$ is secret. The objective of the attacks is to determine the key $k \in K$, where the problem is relied on how to design and develop cryptosystem capable to securely encrypting data by using the properties of these finite fields.

B. Infinite Field Cryptography

New technology and new application bring new threats, and force us to invent new protection mechanisms. There is a growing demand for secure cryptographic techniques.

Since the 1990s, several researchers have observed that there exists an interesting relationship between chaos, fractal and cryptography. Many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems [1]. They are characterized by sensitive dependence on initial conditions, and similarity to random behavior, a part from geometrical and statistical complexity, that explain why this application field qualifies for encryption purposes. 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 [4].

In recent years, many studies on chaos and fractal based cryptosystems have been published. Much work has been done by incorporating chaotic maps into the design of symmetric and asymmetric encryption scheme. In 2003, Kocarev and Tasev [5] proposed a public key encryption algorithm based on Chebyshev chaotic maps. Since then many studies on a new key agreement protocol based on chaotic maps were undertaken [6,7]. There were also proposals for incorporating fractal functions into the design of symmetric and asymmetric encryption schemes using the similar mechanism [8-17]. However though many of the proposed schemes have several advantages such as computational efficiency, ease of generating public-private key pairs etc. Fractal geometry and, in particular, the theory of fractal functions, has evolved beyond its mathematical framework and has become a powerful and useful tool in the applied sciences as well as engineering. The realm of applications includes structural mechanics, physics and chemistry, signal processing, and cryptography. The reason for this variety of applications lies in the underlying complicated mathematical structure of fractal functions, specifically their recursive construction. They provide better approximates for certain problems than their classical non-recursive counterparts. This paper focuses on exposes the reader briefly to the latest application of chaos and fractal functions in cryptography [18].

The strength of cryptography lies in choosing the keys, which are secret parameters, used in encryption. It should not be possible to guess the key by an intruder.

The theory of chaos and fractal is giving us a new way of thinking and new concept of measurements. It looks at the universe in an entirely different way not in Newtonian way but in chaotic way, not using Euclidean geometry but using fractal geometry. A system is called chaotic if it is impossible to make accurate long term predictions about the behavior of the system [19]. Chaotic systems have many perfect dynamical properties, which can be connected with some requirements of a good cipher. Such properties include exponential sensitivity dependent on the initial conditions, leading to a long term unpredictability ergodicity and mixing properties which meet the confusion and diffusion properties required by Shannon.

C. Comparative Study

The most common classical cryptosystems works on discrete finite fields and in discrete time while the crucial point in emerging cryptosystem is the usage of continuous-value systems that may operate in continuous or discrete time. Some special consideration about the similarity and differences between classical and emerging cryptosystem must be taken into consideration to ensure an appropriate design for cryptosystem.

<table>
<thead>
<tr>
<th>TABLE I. COMPARISON BETWEEN FINITE AND INFINITE CRYPTOGRAPHY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Finite field cryptosystems</strong> (Classical cryptography)</td>
</tr>
<tr>
<td>Defined on Integer numbers</td>
</tr>
<tr>
<td>Using algebraic methods based on rounds</td>
</tr>
<tr>
<td>Confusion</td>
</tr>
<tr>
<td>Diffusion</td>
</tr>
<tr>
<td>Statistical analysis is applicable</td>
</tr>
<tr>
<td>Some known attacks is applicable</td>
</tr>
</tbody>
</table>

D. The advantages and drawbacks of finite and infinite set cryptosystems

The encryption schemes that were impractical a few years ago is now possible to implement with the fast development in the computer technology. This developments has a good effect in the cryptanalysis processes also, where the intruder can quickly analyze the intercepted message. So the schemes that might be secure before, now can be broken easily. The widespread use of technology has increased the necessity for encryption.

These motivate us to develop the classical methods that do
not seem to be appropriate for the image security due to some intrinsic features of images such as bulk data capacity, high redundancy, strong correlation among adjacent pixels, etc. To provide a better solution to image security problems, a number of image encryption techniques have been suggested during last one and half-decade. Among them the techniques based on fractals and chaotic dynamical systems provide a good combination of speed, high security, complexity, reasonable computational overheads and computation power, etc [20].

Many properties of fractal and chaotic systems have their corresponding in traditional, with the following point we will point out some advantages and drawbacks of the two disciplines.

1 - Since fractals and chaotic systems have derive their inherent complexity from the extreme sensitivity of the system to the initial conditions, i.e. no closed form solutions exist for them, and therefore “simple” formulas that exactly define the system at any given time do not exist. As applied to cryptography, this qualifies as a very hard problem. The major advantage that chaotic and fractal systems are provably hard, eliminating one of the fundamental drawbacks to conventional encryption.

2 - Since fractals and chaos can change value very dramatically over a short interval, an attacker trying to break a system using fractal and chaos cryptography would have telling when they were “close” to finding the solution to the problem.

3 - The completely deterministic property of the chaos and fractal functions are leads to, we can only obtain the same sets of values provided we have exactly the same function and initial value.

4 - To ensure a complicated structure of trajectories of the dynamical system proposed as the algorithm, we postulate that except of being chaotic, the system should be ergodic or, preferably, mixing. These properties make that our cryptosystem is robust against any reasonable statistical attack and ensure the standard quality of the cryptosystem.

5 - The method of encryption using chaos and fractal cryptosystems does have some drawbacks. Such that it is a symmetric algorithm, which means that key exchange must be handled with a specialized protocol or algorithm. Additionally, the use of floating point arithmetic is slower than integer, this problems have been overcome with the high performance and huge capacities of computers nowadays.

6 - Another weakness of chaos and fractal cryptography is attributed to the lack of proof of security. If we cannot find the weakness in the system, that is not means that the system is secure without prove of its security, or even the prove of its lack of security.

7 - Another weakness of chaos and fractal cryptography is that the system is insecure for encrypting very long messages. We can attribute this weakness to the fact that chaos mappings can repeat, or go into an orbit, for various initial conditions.

III. PERFORMANCE AND SECURITY ANALYSIS

Based on nonlinear fractal functions defined within the infinite subfield (0,1). The main purpose for investigating into this study is to find a system which perform better than what exist currently. The proposed protocol appears to have attractive benefits, due to the properties and complicated mathematical structure of fractal functions with open key space. It possesses sufficient level of security to withstand some known attacks applicable on finite field. They are considered as time consuming to be involved in solving non-linear system numerically over the definite infinite subfield.

First of all, to resist common attacks, the designed cryptosystem should have the following two basic cryptographic properties: confusion and diffusion. The first property is intended to make the relationship between the key and the ciphertext as complex as possible. The second property refers to rearranging or spreading out the bits in the message so that the influence of individual plaintext or key bits is spread out over as much of the ciphertext as possible [21].

Some attackers attempt to break the encryption scheme by making use of image data's properties. For example, they use different key to encrypt or decrypt the same image, and guess the key by investigation the difference between the encrypted or decrypted images. To counter this kind of attacks, high key sensitivity is required, which means that a slight difference in the decryption key will produce a quite different image. In the proposed scheme, the key sensitivity depends on the parameter sensitivity and the cipher's key sensitivity. Since the parameters with high sensitivity are selected, and the cipher with high security is adopted, the encryption scheme's key sensitivity can be confirmed [4].

Different methods have been proposed to attack chaos and fractal based cryptosystems, for both analog and digital settings, to different degrees of success. Since the attacking methods of digital chaotic ciphers are not easy for classification, here we only discuss the analog case. There are three possibilities for cryptanalysis [Beth et al.,1994]:

- Extracting the message signal m(t) directly from the transmitted ciphertext signal c(t).
- Extracting the chaotic carrier signal x(t) to recover the message signal m(t) by removing x(t) from the transmitted ciphertext signal c(t).
- Estimating the secret parameters from the transmitted ciphertext signal c(t) to completely break the whole cryptosystem.

The fractal algorithm is able to withstand the known attacks due to the open key space and big key size. The "cumulative and truncation errors" accompanying the numerical solution of the non-linear system pose a difficulty for the algorithm to obtain imprecise decimal numbers. Based on fractal properties, which ensure a sufficient level of randomness security and randomization of the cryptosystem.

As indicate in Figure(1,2,3) the performance comparison is done in terms of its evaluation parameters, key space and key size between fractal, DSA, and RSA, also among another
digital signature protocols (the GQ and RSA digital signature) that is based on finite field that deals with discrete log and factorization problem. We conclude that the proposed scheme based on fractal function resulted in a better performance compared to the other schemes in term of the execution time under the same environments, and this is an expected result, as the time needed to calculate the decimal number is less than the time needed for integer numbers. The. Figure(4) shows the key space comparison between fractal, DSA, and RSA protocols. Algorithm complexity play the main role in the security of digital signature protocols. Although the three scheme provide equal strength of security, the fractal scheme is more efficient than DSA and RSA schemes, due to fast execution and small key size, which play as an essential factor to ensure the hardness of the problem and to prevent some known attacks. For any chosen number of bits \(n\), the fractal key space includes \(2^n\) possible key values, while the number of possible keys for DSA and RSA is limited to the number of primes in \(\mathbb{Z}_p\) where \(p\) is the largest \(n\)-bits prime. The estimated value of DSA and RSA key space is calculated by \(n=\log n\).

Figure(4) is graphed using the difference equation, 
\[
\text{Diff}=2^n-(2^n/\log(2^n)).
\]
IV. CONCLUSION

In order to present any work in a systematic form to fulfill some basic cryptographic requirement it should pass the main issues: implementation, key management, and security. The main aim of this short study is to discuss a deep relation between two scientific areas: finite and infinite field cryptography. The advantages and the drawbacks are pointed out after some performance comparative study between these two disciplines using some known examples. Security analysis based on some best known attacks are evaluated to conclude that if we cannot find the weakness in the system, that is not means that the system is secure without prove of its security, or even the prove of its lack of security. Another conclusion is chaos and fractal can be applied to cryptographic field and it could generate ciphertext that would be difficult to break.