Commun Nonlinear Sci Numer Simulat 29 (2015) 102–115

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

journal homepage: www.elsevier.com/locate/cnsns

A dynamical systems approach to the discrimination of the modes of operation of cryptographic systems

Jeaneth Machicao[a,1], Jan M. Baetens[b], Anderson G. Marco[a,1], Bernard De Baets[b], Odemir M. Bruno[a,1,*]

[a] Scientific Computing Group, São Carlos Institute of Physics, University of São Paulo, PO Box 369, 13560-970, São Carlos, SP, Brazil
[b] KERMIT, Department of Mathematical Modelling, Statistics and Bioinformatics, Ghent University, Ghent, Belgium

ARTICLE INFO

Article history:
Received 27 September 2013
Revised 16 December 2014
Accepted 19 January 2015
Available online 6 May 2015

PACS:
05.45.Gg
89.70.-a
05.45.-a

Keywords:
Cryptography
Modes of operation
Dynamical systems
Cellular automata

ABSTRACT

Evidence of signatures associated with cryptographic modes of operation is established. Motivated by some analogies between cryptographic and dynamical systems, in particular with chaos theory, we propose an algorithm based on Lyapunov exponents of discrete dynamical systems to estimate the divergence among ciphertexts as the encryption algorithm is applied iteratively. The results allow to distinguish among six modes of operation, namely ECB, CBC, OFB, CFB, CTR and PCBC using DES, IDEA, TEA and XTEA block ciphers of 64 bits, as well as AES, RC6, Twofish, Seed, Serpent and Camellia block ciphers of 128 bits. Furthermore, the proposed methodology enables a classification of modes of operation of cryptographic systems according to their strength.

1. Introduction

The propagation and continuous flow of information are of utter importance for the development of stable economies throughout the world as they are a prerequisite for successful business transactions, short- and long-range communication, and so on [1]. Often this information has to be encrypted in such a way that it can be safely transferred between the sender and recipient without allowing others to read the information that is present in such an encrypted message [2]. On the other hand, malicious persons and organizations, but also governmental organizations, are continuously striving to break the key with which messages were encrypted because this might enable them to get those pieces of information that are needed to achieve their criminal, protective, or other goals [3,4]. It is probably due to the impact of Turing's success in breaking the Enigma that humanity became aware of the importance of cryptography in general, and the vulnerability of ciphers more in particular [5].

Since this major breakthrough, the functioning of the industrial, financial and public sector has become strongly dependent on the advances of cryptography. For instance, while the availability of worldwide networks has enabled rapid dissemination of information, it has also stimulated cryptographic innovations because a significant share of this information may only be

[*] Corresponding author. Tel.: +551633738728.
E-mail addresses: machicao@ifsc.usp.br (J. Machicao), jan.baetens@ugent.be (J.M. Baetens), bernard.debaets@ugent.be (B. De Baets), bruno@ifsc.usp.br (O.M. Bruno).
[1] http://scg.ifsc.usp.br

http://dx.doi.org/10.1016/j.cnsns.2015.01.022
1007-5704/© 2015 Published by Elsevier B.V.

available to a few parties. In this manner, technological progress during the last decades has increased the need for secured communication and transactions, information shielding, and so on [3,4].

In the last few decades, modern cryptography replaced mechanical schemes with new computing models. This modern focus influenced the classical design of ciphers far beyond the original purpose. Nowadays, there are two class of cryptographic algorithms depending on the key: symmetric and asymmetric. Symmetric encryption algorithms use the same key for both encryption of plaintext and decryption of ciphertext. This class of algorithm is also divided into two categories: stream ciphers and block ciphers. Block ciphers have gained wide popularity since the introduction of the first adopted encryption: The Data Encryption Standard (DES) [6], in the mid-1970s, yet nowadays this cipher is considered prone to brute force attacks. To overcome this shortcoming the International Data Encryption Algorithm (IDEA) [7] was designed in 1991 to replace DES. Ever since, there has been a pursuit for the development of new algorithms that meet the rising security expectations. In 1997, the National Institute of Standards and Technology (NIST) [8] selected the official Advanced Encryption Standard (AES) among many competitors, namely Serpent [9], Twofish [10], RC6 [11], Rijndael [12], etc.

To date, block ciphers are the most important elements in many cryptographic systems [3]. A block cipher breaks a message into blocks of elements (bits) and then encrypts one block (*plaintext*) at a time producing its corresponding output block (*ciphertext*). However, a block cipher by itself allows for the encryption of only one block, such that it is recommended to use a mode of operation in conjunction [13]. This mode of operation specifies a mechanism to improve the corresponding block cipher, while encrypting all of the blocks, one by one, as it goes along.

Motivated by the analogies between cryptographic and dynamical systems, on the one hand, and the lack of a means to discriminate between different modes of operation that can be used to encrypt a message with a block cipher using a single key, on the other hand, we demonstrate in this paper how Lyapunov exponents can be relied upon for tackling this problem. More specifically, by contemplating the whole of a cipher, ciphertext and key as an utter discrete dynamical system, *i.e.*, a cellular automaton (CA), and by resorting to the notion of Lyapunov exponents as they have been conceived for such systems [14,15], we show how these measures can be exploited to identify the mode of operation that was used during the encryption process.

Although the cryptographic process of encrypting and decrypting information does not constitute a dynamical system as such, it has been reported that it is possible to draw parallels between cryptographic and dynamical systems [16–19]. Hence, drawing upon such parallels, we have a means to exploit similar tools as the ones that have been conceived in the framework of dynamical systems in order to characterize cryptographic systems. Taking into account that the stability of a dynamical system is generally acknowledged as its main characteristic because it gives insight into its intrinsic nature [20,21], it is natural to verify whether the dynamical systems viewpoint of a cryptographic system allows for a similar notion in order to better understand the latter. An exploration of this is further motivated by the fact that several researchers have noticed a close resemblance between a cryptographic system on the one hand, and a chaotic system, on the other hand [22–25], and the large number of chaos-based cryptosystems [26,27].

Classically, the stability of a dynamical system is assessed by computing its so-called largest Lyapunov exponent that quantifies how it behaves if it is evolved from two different but close initial conditions [20]. Either the corresponding phase space trajectories diverge or converge in which case we refer to the system as unstable or asymptotically stable, respectively, or the system is conservative, which means that the initial separation remains.

As the fields of cryptography and dynamical systems are not yet strongly interwoven, the basic definitions and concepts that relate to those systems and that are of interest within the framework of this paper are presented in Section 2, while the dynamical systems viewpoint on cryptographic systems is presented in Section 3 together with the proposed method for identifying the underlying mode of operation. Finally, the strengths of the proposed method are illustrated and discussed in Section 4 by means of computer experiments.

2. Preliminaries

In this section we introduce the specificities of both cryptographic and dynamical systems that are indispensable for a clear understanding this paper.

2.1. Block ciphers and modes of operation

Classically, an encryption system encloses three major components, namely a cipher, a key, and finally, a ciphertext. The former constitutes a sequence of instructions that must be executed in order to encrypt a given plaintext, which may be envisaged as a sequence of N bits, such that it can be represented as a Boolean vector $\mathbf{P}$ of length N. The result of this encryption process using a key K, which is a sequence of k bits, is a so-called ciphertext, which may be represented in a similar fashion as a Boolean vector $\mathbf{C}$ of length N [3].

Of course, the real plaintext size varies and is mostly different from the length of the blocks for which a block cipher is designed. Consequently, common ciphers cannot be applied directly for the encryption of arbitrary-length plaintext [28]. In order to overcome this issue, so-called block ciphers have been designed and implemented. A block cipher slices the plaintext of length N into b blocks of n bits, after which each of these blocks is encrypted/decrypted by a block cipher, denoted as E_K and E_K^{-1}, respectively. Mathematically, the encryption of a plaintext $\mathbf{P} = (P_1, P_2, \ldots, P_b)$ of length n into a ciphertext of the same length can be formalized as $\mathbf{C} = E(K, \mathbf{P}) = E_K(\mathbf{P})$, where E: $\{0, 1\}^k \times \{0, 1\}^n \to \{0, 1\}^n$. If the length N of the plaintext is not a whole multiple of b, additional bits are padded to the last block of the plaintext.