Nonlinear Dynamics and Systems Theory, **24** (4) (2024) 366–379

Sharing Keys Using Some Toeplitz Matrices and Logistic Maps

Benzeghli Brahim * and Adoui Salah

University of Batna 2, Batna, Algeria.

Received: February 12, 2024; Revised: June 21, 2024

Abstract: In symmetric cryptosystems, we use the same keys to encrypt and decrypt data, our question is how to share this common keys? Using the commutativity of the multiplication of circular matrices and sensibility to initial conditions in chaotic logistic maps through two different channels, we give some new techniques for creating and sharing two keys and use them to increase the level of security during the encryption and decryption of texts or digital images.

Keywords: *Toeplitz matrices; circular matrices; logistic maps; chaos; cryptography; BB84 protocol; Diffie-Hellman protocol.*

Mathematics Subject Classification (2010): 70K55, 37D45.

1 Introduction

The main goal of this work is the creation of two keys through two different channels. For the first key, based on the same techniques as in our previous work [1], we set a $t \in [-1, 1]$ and we create a circular matrix generated by the vector $(a(t), b(t), c(t))$ such that $a = t^2 + 1$, $b = t$ and $c = -t$. This choice is made so that the trace and the determinant of the generated circular matrix are strictly positive, which allows us to calculate the initial parameters of a logistic sequence as follows:

$$\mu = \frac{\det \mathcal{T}}{\det \mathcal{T} + 1} + 3 \quad \textit{and} \quad x_0 = \frac{tr\mathcal{T}}{tr\mathcal{T} + 1}. \tag{1}$$

This choice checks the chaotic case because $\mu \in]3, 4[$ and $x_0 \in]0, 1[$. These two parameters will be shared through a quantum channel by the exchange protocol BB84.

* Corresponding author: mailto:b.benzeghli@univ-batna2.dz