Commun Nonlinear Sci Numer Simulat 19 (2014) 101–111

Contents lists available at SciVerse ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

Pseudo random number generator based on quantum chaotic map

A. Akhshani [a,*], A. Akhavan [b], A. Mobaraki [c], S.-C. Lim [a], Z. Hassan [a]

[a] School of Physics, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia
[b] School of Computer Sciences, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia
[c] University College of Science and Technology (UCST), Orumieh, Iran

ARTICLE INFO

Article history:
Received 1 October 2012
Received in revised form 28 April 2013
Accepted 6 June 2013
Available online 19 June 2013

Keywords:
Quantum map
Pseudo-random number generator
Non-periodicity
Statistical complexity
Cryptography
Differential attack
Quantum key distribution

ABSTRACT

For many years dissipative quantum maps were widely used as informative models of quantum chaos. In this paper, a new scheme for generating good pseudo-random numbers (PRNG), based on quantum logistic map is proposed. Note that the PRNG merely relies on the equations used in the quantum chaotic map. The algorithm is not complex, which does not impose high requirement on computer hardware and thus computation speed is fast. In order to face the challenge of using the proposed PRNG in quantum cryptography and other practical applications, the proposed PRNG is subjected to statistical tests using well-known test suites such as NIST, DIEHARD, ENT and TestU01. The results of the statistical tests were promising, as the proposed PRNG successfully passed all these tests. Moreover, the degree of non-periodicity of the chaotic sequences of the quantum map is investigated through the Scale index technique. The obtained result shows that, the sequence is more non-periodic. From these results it can be concluded that, the new scheme can generate a high percentage of usable pseudo-random numbers for simulation and other applications in scientific computing.

1. Introduction

The nature of randomness has attracted an increasing amount of interest in recent years. Many applications require random input. Sources of random numbers can be broadly divided into two classes. The first of these is the pseudo-random number generators (PRNGs) and the second is true random number generators (TRNGs). The primary difference between random and pseudo-random numbers is that pseudo-random numbers are necessarily periodic whereas truly random numbers are not. Also, pseudo-random number generators are deterministic algorithms. In most of the scientific fields, the first one is particularly desirable feature for some applications, such as simulations of stochastic processes, statistical sampling and performance evaluation of computer algorithms and Monte Carlo simulation. True random number generators are further classified into physical and non-physical. This kind of random number generator is often called non-deterministic random number generator since the next number to be generated cannot be determined in advance. Many true random number generators are relatively slow. This paper is focused on PRNGs.

Cryptography is the art of protecting information from any unauthorized access. The central aim of cryptography is to enable two parties to communicate in a secure manner. Cryptographic methods that do not utilize quantum laws fall under classical cryptography.

* Corresponding author.
E-mail address: a.akhshani@yahoo.com (A. Akhshani).

1007-5704/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cnsns.2013.06.017

Quantum communication, the branch of quantum information provides several examples of communication protocols which cannot be implemented securely only classical communication. The most widely known of these is quantum cryptography, which allows secure key exchange between parties sharing a quantum channel subject to an eavesdropper. The best known protocol of this type is quantum key distribution (QKD). Quantum key distribution involves the communication of a secure cryptographic key between two parties, Alice and Bob, in remote locations by exploiting the laws of quantum mechanics [1]. QKD allows Alice and Bob to make this exchange over a quantum channel, even if it is controlled by the eavesdropper. In fact, Alice and Bob share a pseudo-random number generator that is used to generate a sheared secret key. Bennett and Brassard had provided the first example of the QKD protocol in 1984 [2]. Their protocol is called BB84. Quantum cryptography systems have been demonstrated operating at speeds of up to 1.25 GHz. True random number generators are not available that operate at this speed, so these systems must use pseudo-random number generators [3].

This is an intrinsic weakness in the system because it relies on a random number generator [4]. The NIST system [5], for example, relies on a Mersenne Twister [6] pseudo-random number generator to create Alice's random bits. The Mersenne Twister is computationally fast and is often used for Monte Carlo simulations, but from a security perspective it is considered unsuitable for cryptography because it only requires observation of 624 iterates to determine all of the parameters needed to predict its next output bit [6]. However, the current standard in cryptographically secure random bits is the Blum Blum Shub (BBS) algorithm [7]. The security of the BBS algorithm is based on the difficulty of factoring prime numbers. But quantum cryptography is important precisely because it does not rely on the difficulty of factoring composite numbers, so choosing PRNG based on such condition seems counter-productive.

One obvious solution would be to use a more secure PRNG. Quantum chaos theory seems to be a tool that can be used to improve the quality of pseudo-random number generators. The word quantum chaos refers to quantum systems which in the classical limit show chaotic dynamics. However, the usage of this phrase even for systems like atomic nuclei, which do not possess a classical limit, is now quite wide spread. Also, chaos in systems with discrete phase spaces is called pseudo-chaos or quantum chaos [8]. Besides quantum mechanics, there are examples of pseudo-chaos abound in digital computers, which behave like discrete classical dynamical systems [9,10]. One aim of the field of quantum chaos is the study of quantum versions of classically chaotic systems. As in classical chaos theory, simple chaotic quantum maps [11] have turned out to provide deep insight into the nature of quantum chaos. Quantum maps have been much studied in the last 25 years as convenient toy models of "quantum chaos" [12,13].

In this paper, a novel pseudo-random number generator based on the quantum chaotic map [14] is proposed. In fact, this quantum map is the logistic map with additive noise that arises from the very lowest-order quantum corrections [15,16]. Note that, the PRNG merely relies on the equations used in the quantum chaotic map. To ensure that a random number generator is secure, its output must be statistically proven unpredictable and indistinguishable from a true random sequence. Several tests are used in order to test the randomness of the presented algorithm. These tests include TestU01 [17], DIEHARD [18], NIST statistical test suite [5] and Entropy test suite [19]. To apply statistical random tests such as SP800-22 and DIEHARD, a sufficiently large size of data is required. If the statistical tests are conducted on small size samples, then tests will yield an inaccurate inference. The tests of TestU01 are grouped into three batteries, small crush, crush, and big crush, which are used to test the quality of the proposed PRNG. The new PRNG passed all tests in TestU01 including linear complexity tests that all linear feedback shift-register (LFSR) and generalized feedback shift-register (GFSR)-based random number generators fail (see [17] for more details). Furthermore, in order to pass random number statistical tests, there is no post-processing procedure which makes it an extremely simple generator. The presented quantum based PRNG passes all the standard statistical tests; therefore, it can be used for any application that requires randomness such as cryptographic applications.

Although there exist very powerful and stringent benchmark for testing PRNGs, but the importance of the main statistical characteristics of a chaotic map should be considered. In this vein, a few quantifiers for measuring the main statistical properties of chaotic PRNGs are proposed. They use mainly two kinds of procedures: (1) quantifiers based on information theory [20–22], (2) quantifiers based on recurrence plots [23,24]. The quantifiers based on information theory are Normalized Shannon Entropy and statistical complexity measure [25]. For the quantifiers based on recurrence plots, several measures to quantify the recurrence plots' characteristics are presented [24]. Because of the "small-scale" structures the visual impact produced by the recurrence plot is insufficient to compare the quality of different PRNGs [25].

In this paper, the randomness of the proposed PRNG is successfully verified by statistical complexity and the normalized Shannon entropy. Moreover, in order to the study of non-periodicity in the chaotic sequences of the quantum map, the Scale index analysis based on Continuous Wavelet Transform (CWT) is carried out [26]. Also, the proposed PRNG is highly resistive against different types of attacks such as brute-force attacks and differential attacks.

2. Quantum chaotic map

This section briefly reviews of quantum logistic map. Quantum logistic map is presented by Goggin et al. in 1990 [14]. In their rich work, a kicked quantum system coupled to a bath of oscillators and a logistic map with very lowest-order quantum corrections is derived. In order to studying the effects of quantum correlations on a dissipative system they start with the Hamiltonian of a kicked quantum system coupled to a bath [14]. The operators used were the well-known boson creation ($a^{\dagger}$) and annihilation (a) operators. In fact, the dynamics of a dissipative quantum map which quantum corrections effectively add noise, become more classical as the dissipation (β) increased. The effects of quantum corrections were made by