Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 125 (2018) 576–583

Procedia Computer Science

www.elsevier.com/locate/procedia

6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India

Memristor based Random Number Generator: Architectures and Evaluation

Vikash Kumar Rai, Somanath Tripathy, Jimson Mathew

Department of Computer Science and Engineering
Indian Institute of Technology Patna, Patna 801106, India

Abstract

Security plays an important role in various computer and network applications. Random number generator is a critical component for different cryptographic systems including key generation, unique identification, cookie generation etc. Recently, many architectures using memristor have been proposed for different computing and storage applications. It is observed that memristor based design possesses better randomness. This paper evaluates various memristor based random number generator structures and proposed a new architecture which meets the NIST standards for random number. It is shown that the proposed architecture is cost effective and low power consuming.

Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications

Keywords: random number generator; memristor; NIST

1. Introduction

The arcs of security become more extensive from storing and securing the secret data to creating an environment which is reliable to the user. Security of information and hardware is emerging as a metric of great significance for systems and applications. Random number generators (RNGs) are implemented in many computer applications, specially in security applications, to generate keys, cookie, unique identifications etc [1]. Due to high importance of random numbers, the research field related to random number generation is highly focused by the researchers. Recently, caused by increasing number of attacks and vulnerabilities, the randomness of secret key plays an important role for the security of the applications because greater the randomness of the key, lesser will be the the probability to break the keys.

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000.
E-mail address: vikash.pcs15@iitp.ac.in

1877-0509
Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications
10.1016/j.procs.2017.12.074

There are two main types of random number generators which are true random number generators (TRNGs) and pseudo random number generators (PRNGs). TRNG uses timing jitter, last passage time or multiple threshold crossings. PRNG is easy to implement with linear feedback shift register (LFSR) based structure. Recently, apart from these traditional approaches, people are using memristors in their designs to build random number generators. The prime advantages of using memristors are their compact size, energy efficiency and compatibility with complementary metal-oxide-semiconducter (CMOS) fabrication process.

Wang et al. in [2] have build a 2-branch random number generator with a different architecture. It consists of six transistors and one memristor in each branch. This design uses the stochastic property of the memristors, when memristor switches between its binary states. This increases the randomness of the output. Noor et al. in [3] discussed the use of memristor in ring oscillator based random number generators and proposed an architecture in [4]. This architecture is a five stage memristor based random number generator. Each stage consists of a memristor and a NMOS transistor. They have shown in their simulation that randomness is greater in memristor based random number generator as compared to inverter based because memristor is able to generate highly random output when it is incorporated in circuit designs.

This paper analyzes three different random number generators and proposes a new architecture for random number generation. Our proposed architecture uses memristor to enhance the randomness of the output bit sequence. The National Institute of Standards and Technology (NIST) group of tests are used to determine the randomness of a binary sequence [5]. NIST test has been conducted for all the architectures including our proposed one and found that our architecture performs better than others.

The rest of the paper is organized as follows. Background and related work is included in section II. We discuss our proposed work in section III. Simulation and results are shown in section IV. We conclude the paper in section V.

2. BACKGROUND AND RELATED WORK

Memristor, sometimes also referred as memory resistor, exhibits certain electrical properties and perpetuate a connection between the time integral of voltage and current across two terminals. Memristor has some unique capabilities which makes it a potential candidate to replace CMOS devices. It is a nanoscale device which possesses the controllable and nonlinear electrical behavior and able to generate more randomness than CMOS devices. Also, it requires less area and low power consumption. However, there are many architecture of the memristors have been proposed but the model described in [6] is widely used. This architecture is shown in Figure 1. It consists of an undoped TiO2 layer without oxygen vacancy which is placed below the heavily doped TiO2-x layer with oxygen vacancy. These two layers are kept between a pair of metallic electrodes. The reason behind its popularity is its compatibility with CMOS fabrication process and it is also relatively easy to implement. Memristor can be modeled as a combination of two registors in series. The total resistance of the memristor can be given by following equation:

$$R_{eq}(t) = \frac{w(t)}{d}.R_{on} + (1 - \frac{w(t)}{d}).R_{off} \tag{1}$$

where R_{on} is the device low-resistance when the entire device is doped, and R_{off} acts as the device high-resistance when the entire device is undoped. It has been observed that when $R_{off} \gg R_{on}$, the instantaneous resistance value is calculated by:

$$R_{eq}(t) = R_0 \sqrt{1 - \frac{2\eta\Delta R\phi(t)}{D^2 {R_0}^2}.\mu.R_{on}} \tag{2}$$

where R_0 is equivalent to R_{off}, Δ R= R_{off}- R_{on}, μ is the average ion mobility, $\eta(=\pm 1)$ is the polarity of the applied voltage signal, and the flux ϕ(t) incorporates the history of the applied voltage to the device: