

Daniel Chicayban Bastos
Luis Antonio Brasil Kowada
Raphael C. S. Machado
Instituto de Computação
Universidade Federal Fluminense
Niterói, RJ, Brasil.

October 29th, 2019.

Leopoldo Angrisani
Francesco Bonavolontà
Guest Editors of the Special Issue of Acta IMEKO

Dear Dr. Angrisani and Dr. Bonavolontà,

In response to the recommendation we have received on July 11th 2019 by the TC Board of the 2019 IEEE International Workshop on Metrology for Industry 4.0 and IoT, we have submitted our extended **research paper** to your evaluation. This is an extension of our previous, “Measuring randomness in IoT products”, which focused on IoT applications.

In our new submission, we present a new result which leads us to recommend against the use of the NIST SP 800-22 statistical test suite for testing random number generators, which has the practical impact for anyone using random number generators, thus anyone making direct or indirect use of computer sampling or simulations. The NIST SP 800-22 statistical test suite, last revised in 2010, was designed to test and reject random number generators with poor randomness. Being a very popular software package, researchers using this software package may be getting a false sense of security. You will find our new result on the section “on the insufficiency of the NIST SP 800-22 package”. The section proves NIST SP 800-22 software package is not correctly implemented and shows all the details necessary for reproducing the experiment.

In random number generation, there’s the difficult theoretical question of what is an ideal random number generator which requires answering the question of what is a random sequence. We have accessibly¹ addressed this question in the new section “what is a random sequence?”

The new manuscript is an original extension of the publication on 2019 IEEE International Workshop on Metrology for Industry 4.0 and IoT, it has not been published before and is not under consideration for publication anywhere else. There are no conflicts of interest to disclose.

Sincerely,

D. C. Bastos, L. A. B Kowada and
R. C. S. Machado

¹“If you try to write for the novice, you will communicate with the experts — otherwise you communicate with nobody.” (*Mathematical Writing*, Donald E. Knuth, Tracy Larabee, and Paul M. Roberts, 1987.)