

The impossible problem of randomness certification

Julio César Hernández Castro
Universidad Politécnica de Madrid

Facultad de Informática
Sala de Grados - viernes 4 de abril de 2025 - 17:30
Entrada libre hasta completar el aforo

Resumen:

This talk will cover the main challenges encountered when trying to certify the security of True Random Number Generators (TRNGs), and will show how the common approaches to security certification in other realms don't work in this context. We will present both mathematical and engineering challenges and will, at times, try to sketch a viable answer.

Sobre Julio César Hernández Castro:

Julio Hernandez-Castro recibió su doctorado en informática en 2003, por la Universidad Carlos III de Madrid. En 2009 emigró a UK, donde trabajó en las Universidades de Portsmouth y Kent, donde llegó a ser Professor of Cybersecurity at the School of Computer Science. A mediados de 2023 regresó a España y, más concretamente, a la Universidad Politécnica de Madrid.