mgr inż. Krzysztof Mańk
Wojskowa Akademia Techniczna
Wydział Cybernetyki
Instytut Matematyki i Kryptologii

Gdy testy badają to samo

W trakcie referatu pokażemy, na przykładzie testu serii dla ciągu binarnego i testu entropii Maurer'a dla jednobitowego bloku, jakie niespodzianki pojawiają się, gdy dwa testy badają ten sam aspekt losowości ciągu binarnego. Rozważania te są jednym z kroków do określenia kompletnego zbioru testów losowości, mają na celu określić, czy testy te są równoważne i czy w związku z tym przeprowadzać można tylko ten z nich, który pozwala się efektywniej zaimplementować.