Автор: д.т.н. Б.Я. Рябко

Наименование: Асимптотически наиболее мощный тест для генераторов случайных чисел

Описание.

Генераторы случайных чисел (ГСЧ) находят широкое применение в численных методах, криптографии и многих других областях. В большинстве приложений ГСЧ проверяются, или верифицируются, при помощи статистических тестов. ГСЧ и тесты для них играют важную роль в криптографических системах защиты информации и в настоящее время в России, США, Германии, Японии и целом ряде других стран существуют стандарты на статистические тесты, которые должны использоваться в этих странах в системах защиты информации.

В 2020-2022 автором впервые в литературе было описано семейство тестов, асимптотически наиболее мощных (или, другими словами, оптимальных), см. [1,2].

Предложенные тесты могут использоваться в системах защиты информации для верификации ГСЧ и могут быть включены в гос. стандарт.

Публикации: 1. B. Ryabko Asymptotically most powerful tests for random number generators. Journal of Statistical Planning and Inference, 217 (2022), pp. 1 -- *7.*

2. B. Ryabko. *Statistical Testing of Randomness. 2020 International Symposium. on Information Theory and its Applications. (ISITA,2020, October 24–27, 2020 — Kapolei, Hawai'i, USA (on-line) .*

***Название результата*: Асимптотически наиболее мощный тест для генераторов случайных чисел.**

Автор: д.т.н. Рябко Б.Я.

Описание. Генераторы случайных чисел (ГСЧ) находят широкое применение в численных методах, криптографии и многих других областях. В большинстве приложений ГСЧ они проверяются, или верифицируются, при помощи статистических тестов, в которых проверяется основная гипотеза H0 – ГСЧ порождает последовательность из 0 и 1, подчиняющуюся распределению Бернулли P(0) = P(1) = ½, против H1 = последовательность порождается стационарным эргодическим процессом (или подмножеством из этого класса - например, Марковским процессом). ГСЧ и тесты для них играют важную роль в криптографических системах защиты информации и в настоящее время в России, США, Германии, Японии и целом ряде других стран существуют стандарты на статистические тесты, которые должны использоваться в этих странах в системах защиты информации. Однако важно отметить, что, несмотря на многие сотни публикаций, посвященных данной тематики, «наиболее мощных», или «оптимальных», тестов до работ автора [1,2] не было известно.

Новизна результата. В 2020-2022 автором впервые в литературе было описано семейство тестов, асимптотически наиболее мощных (или, другими словами, оптимальных), см. [1,2].

Значимость результата. Разработкой статистических тестов для верификации ГСЧ занимаются сотни исследователей во всем мире, однако автором впервые построены асимптотически наиболее мощные тесты для альтернативной гипотезы H1 «стационарный эргодический процесс» (ранее были известны такие тесты только для более узких классов (Марковских процессов или его подмножеств).

Практическое применение результата. Предложенные тесты могут использоваться в системах защиты информации для верификации ГСЧ и быть включены в гос. стандарт.

ПУБЛИКАЦИИ:1. B. Ryabko Asymptotically most powerful tests for random number generators. Journal of Statistical Planning and Inference, 217 (2022), pp. 1 -- 7.
2. B. Ryabko. Statistical Testing of Randomness. 2020 International Symposium. on Information Theory and its Applications. (ISITA,2020, October 24–27, 2020 — Kapolei, Hawai'i, USA (on-line).