МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2016 Т. 7 № 2 С. 111–114

УДК 519.254.1+53.082.7

Quantum random number generator

K. S. Kravtsov, S. P. Kulik, I. V. Radchenko

Lomonosov Moscow State University, Moscow

Получено 18.II.2015

Abstract. A quantum random number generator (QRNG) based on a photoeffect as a true random process was proposed and implemented as a stand-alone module. It uses a deterministic post-processing algorithm to overcome physical imperfections of real components. Our minimalistic design of QRNG prevents possible loopholes and makes it suitable for commercial production. The proposed QRNG provides a binary output stream of 1.2 Mbit/s that successfully passes NIST statistical tests.

Keywords: random number generation, quantum random number generator, randomness extractor

Квантовый генератор случайных чисел

К. С. Кравцов, С. П. Кулик, И. В. Радченко

Московский государственный университет имени М. В. Ломоносова, Москва

Аннотация. Описан квантовый генератор случайных чисел (КГСЧ), основанный на истинно случайном процессе фотоэффекта, реализованный в виде отдельного модуля. Для устранения физических нерегулярностей компонент используется детерминистический алгоритм дополнительной обработки получаемых случайных чисел. Наша минималистская схема КГСЧ защищает от возможных утечек информации и пригодна для коммерческого использования. Предлагаемый КГСЧ порождает двоичную выходную последовательность с частотой 1.2 Мбит/сек, которая успешно проходит батарею статистических тестов НИСТ.

Ключевые слова: генераторы случайных чисел, квантовый генератор случайных чисел, случайные числа, извлечение случайности

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 2, pp. 111–114 (Russian)