РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

RU 2018611241

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2018611241

Дата регистрации: **26.01.2018**

Номер и дата поступления заявки:
2017662547 04.12.2017

Дата публикации и номер бюллетеня:
26.01.2018 Бюл. № 2

Автор(ы):
Шабля Юрий Васильевич (RU),
Кручинин Дмитрий Владимирович (RU),
Мельман Вадим Сергеевич (RU)

Правообладатель(и):
Федеральное государственное бюджетное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники» (ТУСУР) (RU)

Название программы для ЭВМ:
Программа «PTA: Primality Test Analyser» для анализа тестов простоты числа

Реферат:
Программа предназначена для анализа тестов простоты числа, построенных на основе новых критериев простоты числа. Генерация критериев простоты числа для анализа может выполняться в программе «PCG: Primality Criterion Generator» благодаря найденным авторами программы свойствам композиции обыкновенных производящих функций, а именно для двух обыкновенных производящих функций с целыми коэффициентами $a(x)=\sum_{i=1}^{k} a_i x^i$ и $b(x)=\sum_{i=1}^{m} b_i x^i$ и композиты $F^n(a,b)$ производящей функции $F(x)$ значение выражения $\frac{1}{n}\sum_{k=1}^{n} F^k(a,b)_n$ целое для всех простых n. Интерфейс позволяет выполнять следующие основные функций программы: загрузка нового критерия простоты для построения теста простоты на его основе; сравнение построенного теста с другим новым или уже известным тестом простоты числа; загрузка чисел для анализа тестов простоты числа из файла, ввод таких чисел вручную или определение промежутка, из которого будут браться числа для анализа; определение среднего, минимального и максимального времени проверки числа тестом простоты; определение ошибки теста простоты; построение графика зависимости времени проверки от размера проверяемого числа. Для работы с программой необходимо иметь установленную систему компьютерной алгебры Maxima, к которой необходимо указать путь в программе. Разработка интерфейса осуществлялась в среде Visual Studio Express for Desktop 2012. Программу можно использовать для анализа тестов простоты числа, основанных на новых критериях простоты числа для поиска простых чисел в криптографии с открытым ключом.

Язык программирования: C#

Объем программы для ЭВМ: 162 354 байт