УДК 004.94, 519.9

Применение распределённых вычислений для анализа алгоритмов шифрования

Хуан Карлос Гонсалез.[1], Эли Торрес Рондон Рей[1], Геворкян М.Н.[1]

[1]Российский университет дружбы народов

Распределенные и параллельные вычисления приобретают все большее значение в связи с массовым появлением многоядерных процессоров, в том числе и на мобильных устройствах. Добровольные распределенные вычисления позволяют эффективно использовать доступные ресурсы и сократить врем простоя полезного оборудования

В данной работе, носящей методический характер, описывается настройка, запуск и тестирование системы распределенного дешифрования на основе открытой платформы BOINC [1] (Berkeley Open Infrastructure for Network Computing). Данная платформа предназначена для организации распределенных вычислений в гетерогенных сетях на большом спектре различных вычислительных устройств, в том числе и мобильных. В основе BOINC лежит клиент-серверная архитектура. Удаленные клиенты присоединяются к серверу, получают фрагменты задания, проводят вычисления и отсылают готовый результат обратно на сервер. BOINC используют многие проекты добровольных распределенных вычислений, такие как SETI [2], Einstein[3].

В докладе на примере четырех протоколов шифрования: DES, 3DES, AES и RC6 описывается настройка платформы BOINC для процесса распределенного дешифрования сообщений и ключей различной длины. Основной внимание уделяется именно работе с платформой BOINC. Целью является подробное освещение процесса написания программы-клиента, предназначенной для взаимодействия с сервером BOINC и настройка сервера заданий.

Литература

1. Официальный сайт BOINC *boinc.berkeley.edu*
2. Официальный сайт проекта SETI@home *setiathome.berkeley.edu*
3. Официальный сайт проекта Einstein@Home *einstein.phys.uwm.edu*