

УДК 50.05.15

РАСПРЕДЕЛЕННЫЕ ВЫЧИСЛЕНИЯ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ С ИСПОЛЬЗОВАНИЕМ JAVASCRIPT

П. С. ЗАЙЦЕВ

Научный руководитель И. А. ЕВСЕЕНКО, канд. техн. наук, доц.
БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ

Распределенные вычисления – это процесс разбиения одной трудоемкой задачи на огромное количество подзадач, которые будут выполняться независимо и одновременно на разных устройствах и по выполнению подзадач агрегироваться в одном месте на сервере.

В контексте данного проекта была выбрана достаточно распространенная и отчасти тривиальная задача – оценка криптостойкости алгоритма хэширования MD5 методом полного перебора. Эта задача достаточно показательна по причине своей алгоритмической сложности и предпосылок к применению параллельных вычислений.

Задача разбивается на множество подзадач или же выводится закон для генерации новой подзадачи на основе имеющихся данных.

Затем этими подзадачами наполняется очередь (она же, стек) заданий. По запросу клиент получает задачу для решения, которая блокируется на определенное время. Если по истечении отведенного промежутка времени решение не вернулось от клиента, задача разблокируется и возвращается в стек. Если клиент решил задачу, то решение проходит стадию проверки и занимает свое место в хранилище данных.

Для демонстрации был написан тестовый проект с серверной частью на ASP.NET MVC и бизнес логикой на Javascript.

Для подбора генерируется случайный набор символов из 36-ти символьного словаря (латинские буквы и цифры) и от него вычисляется MD5 хэш, который и предлагается взломать клиентам. Число различных комбинаций примерно равно 60 млн., при длине слова в 5 символов. Время подбора слова прямо экспоненциально зависит от его сложности и обратно пропорционально от числа компьютеров. Основываясь на полученных результатах, можно сделать следующие выводы: создание распределенных систем позволит получить огромные крайне дешевые вычислительные ресурсы; наиболее оптимальными для распределенных вычислений являются браузеры Google Chrome 26 и последняя версия IE 10; для распределенных вычислений наиболее адаптированы мобильные устройства андроид версии 4 и выше, iPhone 4-5 и телефоны на windows phone 8; применение распределенных вычислений на BlackBerry и остальных телефонах не эффективно, для проверки необходимо определять характеристики на сервере User-Agent и не включать вычисления при неподходящих или неизвестных версиях.