ПРИМЕНЕНИЕ МОБИЛЬНЫХ УСТРОЙСТВ ДЛЯ КРИПТОГРАФИЧЕСКИХ ВЫЧИСЛЕНИЙ

Грачев Я.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Петровский Н.А. – к.т.н.,доцент

Постоянно увеличивающаяся производительность мобильных процессоров и устройств позволяет применять их для более широкого круга задач, в том числе криптографических вычислений. В перспективе неоднородные распределенные вычислительные системы на основе мобильных устройств позволят достичь близкой к x86 архитектуре производительности вычислений.

Вычисление хэш-функции занимает достаточно большое время относительно передачи и обработки необходимых для осуществления этого вычисления данных. Таким образом возможно применение мобильных устройств для осуществления криптографических вычислений. При работе с распределенной неоднородной вычислительной системой, которая основана на множестве мобильных ARM устройств, возможно достижение близкой к x86 производительности [1].

В качестве примера для подтверждения возможности и практического смысла осуществления криптографических вычислений с применением мобильных устройств рассматривается обратная криптографическая задача для хэш-функции MD5. Наилучшим способом является атака по нахождению прообраза – поиск сообщения с заданным значением хэша. Но в действительности такая атака не является практически пригодной, так как на практике она не может быть проведена за разумное время при разумных затратах ресурсов. Поэтому, исключая радужные таблицы, единственным вариантом является коллизионная атака [2]. В качестве мобильных устройств используются Xiaomi Redmi Note 5A (ARM Qualcomm Snapdragon 425), Samsung Galaxy Note II (ARM Samsung Exynos 4412), Nexus 5X (эмулятор, x86 Intel i7-6800k).

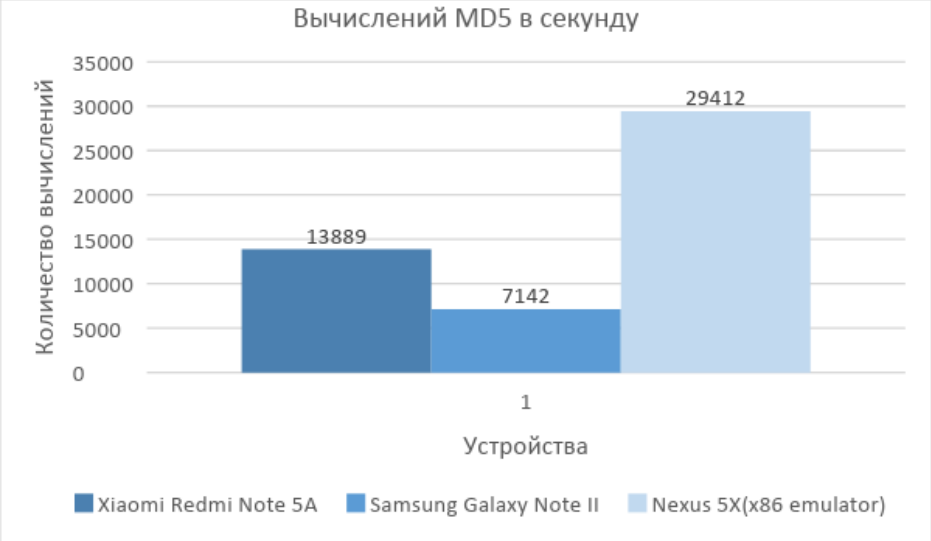

Рисунок 1 – Сравнение вычислений MD5 в секунду для разных устройств

В результате, при анализе количества вычислений MD5 в секунду (рисунок 1) на одинаковых для всех устройств, но разных на каждой итерации, данных наиболее эффективным является эмулируемое устройство на основе x86 процессора, однако современный, но не самый производительный в своем классе, ARM процессор от устройства Xiaomi Redmi Note 5A позволяет считать MD5 хэши всего в 2.1 раза дольше, в то время как более старый Samsung Galaxy Note II еще более значительно уступает x86, но тем не менее показывая положительную и значительную динамику роста производительности ARM устройств и, как следствие, подтверждение возможности и практического смысла осуществления криптографических вычислений на мобильных ARM устройствах, особенно при их объединение в неоднородные распределенные вычислительные системы.

Список использованных источников:

1. Грачев, Я. Ю. Неоднородная распределенная вычислительная система / Я. Ю. Грачев // Компьютерные системы и сети: материалы 54-й научной конференции аспирантов, магистрантов и студентов, Минск, 23 – 27 апреля 2018 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2018. – С. 58 - 59.

2. Rogaway, P. Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. Fast Software Encryption / P. Rogaway, T. Shrimpton. – Berlin; Springer-Verlag. 2004, – 371-388 p.

PLACE – ЛЕГКИЙ ПОИСК ПАРКОВОЧНЫХ МЕСТ

Деменковец Д.В., Прудников В.М., Ивончик К.С., Бондарь Е.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Леванцевич В.А. – ст. преподаватель

Цель данной работы заключается в решении проблемы поиска парковочных мест. В ходе работы было разработано мобильное приложение, которое обладает достаточным функционалом для поиска свободного парковочного места. Кроме этого, программное средство позволяет всегда быть в курсе того, что происходит с автомобилем в текущий момент времени.

В наши дни парковка автомобилей во дворе, у дома или офиса становится проблемой не меньшей, чем городские пробки. Многие, подъезжая домой, вынуждены искать свободное место в своем или соседних дворах. Это отнимает немало времени.

На данный момент в Минске приблизительно 940 тысяч автомобилей. Кроме этого, еще примерно 5-6 тысяч приезжают в город. Однако, по статистике, парковочных мест гораздо меньше. Пользователи автомобилей не очень любят платить за место на платной парковке, и, к сожалению, они не всегда находятся рядом. По статистике каждый водитель тратит примерно 5-10 минут своего времени для поиска парковочного места. Если учесть факт того, что мы это делаем примерно 2 раза в день, то за год в сумме может составить около 70-80 часов.

Для решения данной проблемы было разработано приложение Place, которое обеспечит легкий поиск парковочных мест, надежную систему безопасности, а также навигацию до свободного места на парковке.

Система состоит из следующих компонентов: одна или несколько камер, установленных так, чтобы просматривать всю территорию парковки; маршрутизатор, который отвечает за связь с интернетом; сервер, который принимает данные о местоположении и уровне доступа пользователей; и, непосредственно, само мобильное устройство.

После того, как пользователь выберет нужное ему место парковки, данные о его местоположении и правах доступа будут отправлены на сервер, где из всего множества видеопотоков, ему будут отправлены те, которые он запросил. Далее, на экране своего смартфона пользователь сможет увидеть трансляцию с парковки в реальном времени, убедиться в наличии свободного места, проложить маршрут и двигаться в заданном направлении.

После добавления технологии искусственного интеллекта в приложение, появится возможность проложить маршрут к свободному парковочному месту. Также появится возможность подсчета и выделения парковочного места, а также подсчитать их количество.

Установив мобильное приложение на свой смартфон, пользователь будет иметь возможность оформить платную подписку для пользования данной системой. При входе в приложение пользователь сталкивается с простым и интуитивно понятным интерфейсом, который включает в себя 3 секции:

1) карта с доступными ему парковками;
2) обзор ближайшей от текущего местоположения доступной парковки;
3) навигация до выбранной парковки.

Таким образом, разработанная система позволит заблаговременно оценить ситуацию на парковке и целенаправленно двигаться к свободному месту, используя встроенную систему навигации в приложении. При этом, пользователь сэкономит время и нервы, которые он мог потратить на поиск незанятого места. С точки зрения безопасности, система Place позволит всегда быть в курсе того, что происходит с вашей машиной в режиме реального времени

Дополнительно приложение может способствовать разгрузке дворов. Place поможет заранее определить, есть ли свободные места во дворах и стоит ли туда ехать. Увидев на экране своего смартфона, что все парковочные места уже заняты, водитель может попытаться найти иное свободное парковочное место. Администрация города также будет заинтересована в разгрузке дворов. Коммунальные и экстренные службы смогут более эффективно работать.

Список использованных источников:

1. Documentation for app developers [Электронный ресурс] // developer.android.com : Сайт разработчика URL: https://developer.android.com/docs(дата обращения: 19.12.2018).

2. Apple Developer Documentation [Электронный ресурс] // developer.apple.com : Сайт разработчика URL: https://developer.apple.com/documentation/(дата обращения: 21.12.2018).

3. Escam [Электронный ресурс] // escam.cn : Сайт разработчика URL: http://www.escam.cn/(дата обращения: 05.02.2019).

4. В. Олифер, Н. Олифер. Компьютерные сети. Принципы, технологии, протоколы. 4-е издание. [Электронный ресурс] // rulit.me : Сайт разработчика URL: https://www.rulit.me/books/komryuternye-seti-principy-tehnologii-protokoly-read-467113-1.html(дата обращения: 14.12.2018).