считывателя к другому компьютеру. Это позволяет произвести настройку или конфигурирование считывателя на одном компьютере, а эксплуатировать – на другом компьютере. Используемое программно-аппаратное оборудование соответствовало основному действующему стандарту ISO/IEC 18000-2:2009. Дистанция регистрации обычно составляла 10 ~ 50 мм. Оборудование близкого чтения недорого, но сами метки являются относительно дорогими и без перспектив удешевления из-за конструктивных особенностей их изготовления.

ИСПОЛЬЗОВАНИЕ ВЕРОЯТНОСТНЫХ СТРУКТУР ПРИ РАБОТЕ С БОЛЬШИМИ ОБЪЕМАМИ ДАННЫХ

И.Е. Закревский

Операции над большими массивами данных являются неотъемлемой частью ежедневной работы. Растут базы данных, что сказывается на скорости работы средств защиты информации, таких как средства аутентификации, DLP системы, анализаторы трафика и т.д. Одним из путей решения проблем скорости доступа является использование вероятностных структур данных, в частности – фильтр Блума.

Фильтр Блума – это вероятностная структура данных, позволяющая хранить и проверять принадлежность элемента к множеству [1]. В фильтре Блума возможны ложноположительные срабатывания. Фильтр Блума представляет собой битовый массив из m бит, которые по умолчанию обнулены. Далее, пользователю необходимо определить k независимых хеш-функций, которые будут преобразовывать массив входных данных произвольной длины в битовую строку фиксированной длины m достаточно равномерным способом. Процент ложноположительных может быть уменьшен увеличением размера массива m и/или числа хеш-функций k [2].

В данной работе был реализован фильтр Блума ($k = 3$, $m = 109$) и использован для определения необходимости вызова удаленной БД. Использование фильтра Блума в качестве структуры данных для хранения информации о наличии элемента в БД позволило сократить на 77 % используемую память по сравнению с хеш-таблицами, также незначительно уменьшило время на добавление состояния новых элементов в множество (> 5 %).

Литература

1. Bloom, B.H. Space/time trade-offs in hash coding with allowable errors.
2. Dillinger, P.C. Fast and Accurate Bitstate Verification for SPIN.

РАЗРАБОТКА ПРИЛОЖЕНИЙ ДЛЯ БЕЗОПАСНЫХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ НА ОСНОВЕ ГОМОМОРФНОЙ КРИПТОГРАФИИ И ОЦЕНКА ИХ ЭФФЕКТИВНОСТИ

М.А. Кадан

С внедрением повсеместного использования облачных технологий остро встает вопрос сохранности данных и их безопасной обработки в облачных хранилищах. Разумным решением проблемы обеспечения конфиденциальности данных может служить шифрование всех приватных данных перед передачей в облако и обеспечение выполнения операций над зашифрованными данными, без их предварительного дешифрования, известное как гомоморфное шифрование [1].

Предметом доклада является применение гомоморфного шифрования в реализации безопасных мобильных приложений для облачных вычислений. Рассматривается задача определения требований к безопасности использования облачных хранилищ данных и подходов к проведению безопасных вычислений над данными облачного хранилища с использованием методов гомоморфного шифрования [2].

На основе теоретических принципов гомоморфного шифрования обоснован, спроектирован и реализован модуль для обеспечения возможности безопасного хранения и обработки данных в облачных структурах, не имеющий аналогов для решения задач данного рода на платформе iOS. Исследована эффективность использования метода гомоморфного шифрования в зависимости от максимальной длины операндов и ключа шифрования, а также исследована производительность модуля с использованием приложения на языке Swift.