

## **ПОДДЕРЖКА DIGITAL RIGHTS MANAGEMENT В МОБИЛЬНЫХ УСТРОЙСТВАХ НА БАЗЕ ANDROID**

П.В. САВЧЕНКО, Е.Р. ПЕЛЬКИН

Возросшая популярность мобильных устройств под управлением системы Андроид, ставит перед пользователем компьютерной техники новые проблемы. Одна из них, для многих достаточно важная, это защита информации на мобильных устройствах под управлением Андроид.

Большинство DRM решений построены по единой архитектуре. Защищаемый контент предварительно шифруется DRM модулем шифрации (как правило, применяется AES-128), а модуль управления лицензиями выдает ключи пользователям на просмотр контента (как правило создается на базе Java сервера приложений). Такая реализация позволяет эффективно разделить этапы обработки контента, доставки контента и управления разрешениями на использование.

В случае Android системы защиты контента приложение берет на себя лишь дешифрацию данных получаемых по HTTP Live Streaming протоколу при помощи заранее указанного ключа дешифрации. В качестве алгоритма используется стандартный AES-128. в этом случае разработчику приложения нужно реализовать на серверной части механизм сохранения ключей шифрации и очень аккуратной их выдачи, а на клиентской части обеспечить качественный прием этих ключей с минимальным риском для перехвата (например, обеспечить jailbreak detection в приложении).

При доставке ключей в приложение для защиты ключей предлагается использовать HTTPS. При этом остается риск перехвата ключа, в тех случаях если произвели взлом устройства (Jailbreak) или каким-то образом сэмулировали на PC данное устройство. Существенно снизить этот риск, можно лишь при написании своего приложения, реализовав дополнительные проверки.

## **НЕРАВНАЯ ЗАЩИТА ДАННЫХ ПРИ ПОМОЩИ НЕРАВНОМЕРНОГО ДВУМЕРНОГО КОДИРОВАНИИ ИНФОРМАЦИИ**

НЕСТОР АЛЬФРЕДО САЛАС ВАЛОР

Известны многие алгоритмы декодирования двумерного неравномерного кодирования информации. Одним из них является алгоритм на основе нахождения на предварительном этапе обработки кодеком данных всевозможных комбинаций размещения ошибок определенной кратности  $t_i$  в сжатой форме. Все эти образы ошибок формируют общую библиотеку образов ошибок и для каждого образа формируются правила идентификации ошибок соответствующей кратности. Известна библиотека образов ошибок для неравномерного совместного способа кодирования информации. Однако, данный способ кодирования и декодирования информации неэффективен и сложен в реализации при коррекции многократных ошибок.

Для устранения данных недостатков предложен метод формирования библиотеки образов ошибок на основе двумерного равномерного кодирования информации. Установлено, что при данном способе кодирования и декодирования общее число образов трехкратных и четырехкратных ошибок уменьшается примерно на 32% и 18% соответственно по сравнению с использованием библиотеки образов ошибок при неравномерном совместном кодировании и декодировании информации. Уменьшение общего числа образов обеспечиваются за счет исключения из

библиотеки образов ошибок таких размещений ошибок по зонам, которые превышают корректирующую способность кодов в данной зоны.

## **МЕХАНИЗМ ПРОВОДИМОСТИ МДМ-СТРУКТУР НА ОСНОВЕ АНОДНЫХ ОКСИДНЫХ ПЛЕНОК, СОДЕРЖАЩИХ ИТТРИЙ**

С.М. САЦУК, М.М. ПИНАЕВА

МДМ-структуры находят широкое применение при создании различных компонентов для систем защиты информации.

В данной работе представлены результаты исследований нанотонких анодных оксидных пленок, содержащих иттрий, сформированных при напряжении 160 В. в качестве верхней обкладки использовался алюминий или тантал. Часть МДМ-структур подвергалась термообработке при температуре 673 К в течение 3 ч.

Анализ вольт-амперных характеристик МДМ-структур позволяет выделить на них два основных участка: омический (проводимость не зависит от напряженности электрического поля) и неомический. Омический участок, где рост тока пропорционален росту напряжения, наблюдается как при положительно, так и отрицательно смещенной структуре. Напряжение, соответствующее переходу от омического участка к неомическому, зависит от режима формирования нанотонкой анодной оксидной пленки. Отжиг также влияет на напряжение перехода, которое уменьшается с 27 до 22 В. Такому уменьшению напряжения перехода соответствует снижение проводимости структур в 12 раз. Материал верхнего электрода (алюминий или тантал) не влияет на характер зависимостей ток-напряжение.

Анализ литературных данных, касающихся основных механизмов проводимости на постоянном токе МДМ-структур, позволяет выделить три возможных механизма, ответственных за перенос носителей заряда в исследуемых МДМ-структурах: ток, ограниченный пространственным зарядом, эмиссия Пула-Френкеля и Шоттки.

Четко выраженные линейные участки на вольт-амперных характеристиках, их незначительная температурная зависимость и отсутствие влияния материала верхнего электрода всех структур, дают основания считать, что процессы переноса носителей заряда в исследуемых структурах объясняются действием объемных, а не приэлектродных эффектов.

## **СВОЙСТВА АНОДНЫХ ПЛЕНОК НА АЛЮМИНИИ СОДЕРЖАЩИХ РЕДКОЗЕМЕЛЬНЫЕ МЕТАЛЛЫ**

С.М. САЦУК

Свойства анодных оксидных пленок в существенной степени влияет на поглощающую способность диэлектрика в различном диапазоне частот.

Для определения оптимальных условий формирования бездефектных анодных оксидных пленок на алюминии, содержащих иттрий, были проведены исследования их морфологии и профиля распределения анионов электролита.

Морфологический анализ пленок, полученных при напряжении формовки до 160 В показал, что они не содержат дефектов в виде сквозных пор или трещин, а их поверхность имеет вид, характерный для плотных пленок. На анодных оксидных пленках, сформированных при 160 В поры обнаруживаются в очень малых