информационными технологиями при выполнении лабораторных работ и проведении мероприятий по контролю успеваемости.

Значительное внимание при изучении дисциплины уделяется активным методам преподавания, которые подразумевают проведение деловых игр для моделирования поведения современного технического специалиста в реальных рабочих ситуациях, использование виртуальных компьютерных средств и других современных учебно-методических средств. Например, в процессе проведения практических занятий предлагается разработка виртуальных средств измерений (по направлениям), получение измерительной информации в виде отношений с последующим использованием ее в учебной базе данных, разрабатываемой при проведении лабораторных занятий.

Итогом изучения дисциплины «Безопасность баз данных» является самостоятельно выполненный индивидуальный проект, в котором обеспечивается многоуровневая защита разработанной базы данных, устанавливается проверку поддержки целостности данных.

СПИНТРОННЫЕ ЭЛЕМЕНТЫ РЕЗИСТИВНОЙ ПАМЯТИ

М.В. Ремизевич, А.Л. Данилюк

В настоящее время устройства резистивной памяти с произвольной выборкой (RRAM) активно разрабатываются. В перспективе они могут заменить магнитную память (MRAM). Однако еще существует ряд нерешенных проблем, связанных как с пониманием физического механизма переключения сопротивления в электрическом поле, так и с воспроизводимостью параметров элементов памяти. Наноструктуры на основе диоксида гафния перспективны для использования в энергонезависимой резистивной памяти. Оксид гафния имеет высокую диэлектрическую проницаемость, относительно высокую энергия запрещенной зоны и образует термодинамически устойчивый интерфейс с кремнием. Электрический пробой диэлектрика приводит к переключению в состояние с низким сопротивлением и созданию высокой плотности ловушек, что делает возможным долговременное хранение заряда (до 10^6–10^7 с) [1]. Практические результаты состоят в получении стабильных наноразмерных слоев диоксида гафния, переключаемых низким потенциалом. К наиболее важным задачам относится выявление особенностей, связанных с механизмом переключения диоксида гафния из состояния с высоким сопротивлением в состояние с низким сопротивлением. Одна из таких особенностей связана с наличием случайного телеграфного шума, возникающего при электроформовке диоксида гафния. Особый класс элементов памяти и логики составляют спиновые аналоги элементов резистивной памяти, в которых переключение сопротивления обусловливается наличием обратимого электрического пробоя и наблюдается усиление мемристорного эффекта [2, 3].

В данной работе, исходя из гипотезы о бистабильном характере ловушечных состояний, представлены результаты моделирования переключения бистабильных ловушечных состояний в элементах резистивной памяти при наличии поляризованного по спину тока. Приводятся результаты анализа влияния инжекции спин-поляризованного тока на время переключения сопротивления и параметры бистабильных ловушечных центров.

Список литературы

1. F. Pan [et al.] // Materials Science and Engineering R. 2014. Vol. 83. P. 1–59.
2. B.Li [et al.] // Organic Electronics. 2010. Vol. 11. P. 1149–1153.
3. M. Prezioso [et al.] // Advanced Materials. 2013. Vol. 25. P. 534–538.

ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ НА ОСНОВЕ СТОХАСТИЧЕСКОГО ГЕОМЕТРИЧЕСКОГО ПОДХОДА

С.Б. Саломатин, Аль-Эзайрджави Атир Абдулзахра Салах

Стохастическая геометрия используется для изучения показателей безопасности физического уровня беспроводных сетей с подслушивающим каналом передачи. Топология

сети предполагает, что легитимные пользователи и подслушивающие аналитики случайным образом расположены на большой географической территории в соответствии с некоторыми вероятностными распределениями.

Рассматривается децентрализованная беспроводная сеть в двумерном пространстве на основе гомогенной модели однородного точечного пуассоновского процесса PPP. Местоположения легитимных передатчиков соответствуют однородному PPP с интенсивностью λ. Каждый передатчик имеет предполагаемый приемник на фиксированном расстоянии r в случайном направлении [1, 2].

Определяются следующие основные показатели системы защиты.

Граф защищенности. Используется для изучения свойств связности среди легитимных пользователей сети и характеризует существование связи с полной защитой между любыми двумя легитимными пользователями.

Пропускная способность защищенной сети. Учитывает одновременные передачи между всеми допустимыми линиями связи и дает математически поддающийся измерению показатель достижимой пропускной способности сети с заданным требованием защиты на основе перколяционной модели.

Отключение соединения. Событие, когда пропускная способность канала от передатчика для предполагаемого приемника ниже скорости кодового слова. Вероятность этого события называется вероятностью отказа соединения, обозначается как Pco

Сбой в работе системы защиты. Событие, когда пропускная способность канала от передатчика, по крайней мере, к одному перехватчику превышает структурную избыточность. Вероятность того, что это событие произойдет, называется вероятностью отключения секретности, обозначаемой как Pso.

Список литературы

1. Franceschetti R. Random Networks for Communication: from Statistical Physics to Information Systems. Cambridge University Press, 2008.

2. Vaze R. Random Wireless Networks, Cambridge University Press, 2015.

РЕШЕТЧАТАЯ КРИПТОСИСТЕМА НА ОСНОВЕ МНОГООБРАЗИЯ БАЗИСОВ

С.Б. Саломатин, В.В. Панькова

Криптографические механизмы используют библиотеки решетчатого кодирования с масштабируемой реализации примитивов гомоморфного преобразования [1, 2].

Базовая структура решетчатых криптосистем соответствует архитектуре криптосистемы Мак-Элиса с секретной функцией на основе решеток [3]. Исходная криптосистема описывается следующим образом:

Генерация ключей. Формируется удобный с вычислительной точки зрения базис решетки R. Базис R преобразуется в трудно обратимый базис Q с помощью унимодулярного преобразования.. Базис Q используется в качестве открытого ключа (открытого базиса), а базис R – в качестве секретного ключа шифрования (закрытого базиса).

Процедура зашифрования. Выбирается любой вектор решетки **w**, используя открытый базис Q, и к нему добавляется вектор открытого текста **p**. Вектор $\mathbf{c} = \mathbf{w} + \mathbf{p}$ представляет собой зашифрованный текст.

Расшифрование. Используя закрытый базис, решается задача вычисления ближайшего вектора решетки **nw** к зашифрованному тексту **c**. Найденный ближайший вектор решетки **nw** вычитается из зашифрованного текста для получения открытого текста $\mathbf{p} = \mathbf{c}–\mathbf{nw}$.

Безопасность криптосистемы основывается на следующих трех предположениях. Легко вычислить неудобный базис Q из базиса R, но вычислительно трудно решить обратную задачу. Легко создать случайный вектор решетки даже с неудобным базисом Q. Легко найти ближайший вектор с удобным базисом R, но трудно это сделать с открытым базисом Q.

Дополнительное усиление системы состоит в использовании нормальной формы Эрмита для базиса открытого ключа, базисов генераторных матриц алгебро-геометрических структур и построения семейств PRF на основе решеток, через задачи обучения с ошибками (LWE).