любых новых устройств вне зависимости от прав пользователя, ведущего в данный момент сеанс работы.

Проведя исследование, определив возможные угрозы и уязвимости было принято решение о создании устройства, обеспечивающего защиту от программных кейлоггеров, работающих в операционной системе. На базе микроконтроллера Arduino организованы приём событий от физической клавиатуры, модификация этих данных и последующая передача операционной системе. Подготовленное программное обеспечение, работающее в операционной системе, в свою очередь, проводит обратную модификацию и передаёт введённые пользователем данные в защищаемое приложение. Таким образом, данные, которые поступят в кейлоггер, будут находиться в модифицированном виде.

БЕЗОПАСНОСТЬ BLUETOOTH УСТРОЙСТВ

В.А. Кузьменко

Цель исследования — оценить безопасность передачи данных по Bluetooth.

В процессе исследования было выявлено следующее:

– передача данных по Bluetooth защищается PIN кодом на устройствах, поддерживающих Bluetooth версии 2.0 и выше.

– данные шифруются 128-битным AES алгоритмом на устройствах, поддерживающих Bluetooth версию 4.0 и выше.

– устройства инициируют пересопряжение, если на частоту, в которой они работают, начинает влиять неизвестный пользователь. Однако если нет свободных частот в диапазоне Bluetooth, то имеется возможность «подслушать» ключ сопряжения и методом подбора взломать PIN код.

Таким образом, сформирована рекомендация пользователям: в случае использования технологии Bluetooth для передачи данных, требующих шифрование, необходимо самостоятельно осуществлять шифрование таких данных.

Также в ходе исследования было разработано приложение, обеспечивающее безопасность рабочего места персонального компьютера на основе контроля наличия рядом ключевого Bluetooth устройства. Данное приложение позволяет также удаленно подавать команды управления с мобильного телефона на компьютер в зашифрованном виде. При разработке приложения использовалось программно-аппаратное средство для построения систем автоматики и робототехники — Arduino.

АППАРАТНЫЕ РЕАЛИЗАЦИИ ОПЕРАЦИЙ УМНОЖЕНИЯ В ПОЛЯХ ГАЛУА ПРИ ПОСТРОЕНИИ ЭЛЕМЕНТОВ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Е.В. Листопад

При построении современных систем на кристалле (в том числе для криптографической защиты информации) часто возникают задачи реализации арифметических операций в полях Галуа. От эффективности их реализации (в первую очередь, операций умножения) существенно зависят характеристики создаваемых систем. Поля Галуа характеризуются двумя параметрами: число двоичных разрядов, необходимых для представления символа, и генерирующий полином, определяющий порядок следования элементов поля [1].

Рассмотрим аппаратные реализации умножения элементов поля с числом двоичных разрядов равным 16. Умножение в поле подразумевает выполнение двух стадий: логическое умножение и приведение по модулю генерирующего полинома. Выполнение данных стадий возможно в следующих вариантах:

1. Выполнение приведения по модулю после умножения одного из множителей на каждый бит, каждую пару бит или каждые 4 бита второго множителя. Вся операция умножения будет выполнена за 16, 8 или 4 такта процессора соответственно.

2. Выполнение приведения по модулю (на 2-м такте) после перемножения элементов поля (на 1-м такте). Вся операция умножения будет выполнена за 2 такта.

3. Выполнение приведения по модулю на том же такте, что и перемножение элементов поля. Вся операция умножения будет выполнена асинхронно за 1 такт.

Лучшие соотношения показателей быстродействия и аппаратных затрат кристалла имеет вариант реализации умножения за 2 такта процессорного времени.

Литература
1. Поляков А., Тайлеб М., Тайлеб Н. // Современная электроника. 2007. № 5. С. 46–48.

ОПТИМИЗАЦИЯ КОНСТРУКТИВНО-ТЕХНОЛОГИЧЕСКИХ ПАРАМЕТРОВ ЭЛЕМЕНТНОЙ БАЗЫ РАДИАЦИОННО-СТОЙКИХ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

И.Ю. Ловшенко, О.В. Дворников, В.Р. Стемпицкий

Развитие элементной базы специального назначения требует реализации особых подходов к проектированию и исследованию характеристик данной группы полупроводниковых приборов. Моделирование воздействия дестабилизирующих факторов на этапе проектирования ИМС позволяет сократить время проектирования изделий микроэлектроники, а также исправить допущенные ошибки еще до изготовления опытных образцов. Программный комплекс компании Silvaco [2] обеспечивает возможности моделирования электрических и других характеристик ИМС с учетом влияния ионизирующих излучений и экстремальных режимов эксплуатации.

При моделировании технологического процесса формирования структуры полевого транзистора, управляемого p-n-переходом, выделено 14 этапов: задание подложки и расчетной сетки, последовательное формирование областей N^+-скрытого слоя, P^+-скрытого слоя, проведение эпитаксии, формирование оксидной изоляции, областей P-канала, N-коллектора, P^+-коллектора, P-базы, вскрытие областей под контакты, формирование областей N^+-затвора, P^+-эмиттера, N^+-эмиттера, металлизации.

Для полученной приборной структуры построены графики зависимости тока стока от напряжения на стоке при напряжении на затворе 0 В и от напряжения на затворе при напряжении на стоке –3 В. Полученные графики имеют достаточную согласованность с результатами натурных экспериментов (максимальное отклонение по току — 6,32 %, по напряжению отсечки — 1,13 %). Установлено, что наибольшее влияние на электрические характеристики приборной структуры, оказывают технологические операции формирования областей P-канала и N^+-затвора, варьируя параметры которых (доза и энергия имплантации, время и температура отжига) установлена требуемая термостабильная точка ($U_З$ = 0,6 В).

Исследования финансируются в рамках выполнения заданий 3.1.02 и 3.2.01 ГПНИ «Фотоника, опто- и микроэлектроника».

ОПТИМИЗАЦИЯ ХАРАКТЕРИСТИК ПОЛЕВОГО ТРАНЗИСТОРА, УПРАВЛЯЕМОГО P-N-ПЕРЕХОДОМ С УЧЕТОМ НИЗКОТЕМПЕРАТУРНЫХ ЭФФЕКТОВ

И.Ю. Ловшенко, О.В. Дворников

Подвижность носителей заряда в полупроводниках зависит от температуры, так как при разной температуре преобладает тот или иной тип рассеяния носителей заряда. Эффект «вымораживания» примесей при использовании статистики Ферми–Дирака описывается посредством введения коэффициентов, учитывающих вырождение зоны проводимости и валентной зоны.

Моделирование зависимости электрических характеристик структуры полевого транзистора, управляемого *p-n*-переходом, от температуры проводилось в программном комплексе компании Silvaco, который поддерживает большое количество моделей переноса носителей заряда, учитывающих зависимость параметров полупроводников от температуры.

Модель Клаассена в обобщенном виде описывает подвижности основных и неосновных носителей заряда. Она включает эффекты рассеяния на решетке, рассеяния на примесях (с экранировкой от заряженных носителей), рассеяния носителей на носителях и кластеризации атомов примесей при высоких концентрациях. Эта модель применима в интервале температур от 70 до 500 K. Модель Клаассена учитывает более широкий ряд эффектов и откалибрована для более широкого диапазона условий по сравнению с другими моделями подвижности при низком поле.

Экспериментальные измерения показали, что снижение температуры до 143 K приводит к увеличению тока стока полевого транзистора, управляемого p-n-переходом. Однако при температуре ниже 143 K величина тока стока начинает уменьшается. Результаты исследований указывают, что наибольшее соответствие расчетных и экспериментальных данных обеспечивается при применении аналитической модели подвижности и модели подвижности Классена.

Исследования финансируются в рамках выполнения заданий 3.1.02 и 3.2.01 ГПНИ «Фотоника, опто- и микроэлектроника».