от 200 до 240 нм. Расстояние между соседними пиками изменяктся от 230 до 260 нм. Высота столбиков зависит от режимов повторного анодирования. Она увеличивается с ростом напряжения формовки. При напряжении 160 В она составляет 100…130 нм, при 200 В — 130…160 нм, при 240 В — 160…200 нм. Структуры, в которых не проводилось повторное анодирование, имеют высоту столбиков до 100 нм. Таким образом, было установлено, что объемный рост оксида тантала в поры Al_2O_3 линейно зависит от напряжения реанодирования с аспектным соотношением 0,73 нм/В. Показана возможность формирования столбиковых структур с заданными параметрами.

ЭКРАНИРУЮЩИЕ ХАРАКТЕРИСТИКИ ТЕКСТИЛЬНЫХ МАТЕРИАЛОВ С ПОКРЫТИЯМИ

В.Н. КОХНЮК, Б.ДЖ.КОТИНГО, А.М. ПРУДНИК

Всё более распространена проблема несанкционированного доступа к различной информации. Для снижения риска доступа третьими лицами к личной или секретной информации применяются различные способы её защиты. Одним из таких методов является экранирование.

Экраны электромагнитного излучения (ЭМИ) изготавливаются из различных материалов и по различным технологиям. Одной из существенных характеристик экранов, помимо поглощения, отражения и ослабления ими ЭМИ, является их масса. Это обусловливает удобство работы с такими экранами, меньшую материалоёмкость и, следовательно, стоимость экрана при прочих равных параметрах. В последнее время для снижения веса в качестве основы для создания экранов ЭМИ исследуется вопрос использования текстильных материалов с различными покрытиями.

В ФТИ НАН Беларуси проводится нанесение на текстильную основу (из хлопкополиэфирной, льняной, полиамидной, хлопчатобумажной тканей) различных металлов (Ti, Cu, сплава Fe–Cr–Ni), при остаточном давлении 5×10^{-3} Па и в среде реакционно-способного газа CO_2. После нанесения покрытий в НИЛ 5.3 НЧ БГУИР с использованием панорамного измерителя коэффициентов отражения и передачи SNA-0,01–18 измеряются экранирующие характеристики образцов экранов в диапазоне от 0,7 до 17 ГГц.

Измерялись величины коэффициентов отражения и передачи. Для образцов, полученных с применением CO_2, измеренные значения коэффициентов отличаются от значений коэффициентов образцов, полученных в вакууме, на 0,3–1,0 дБ. Так для полиамидной ткани с покрытием из меди коэффициент отражения составил от –1,5 до –3,5 дБ, а с покрытием из меди, осаждённой в среде CO_2 — от –1,2 до –12,8 дБ. Коэффициент передачи для полиамидной ткани составил от 0 до –0,7 дБ для образцов с медным покрытием и от 0 до –0,5 дБ для образцов, полученных с применением CO_2.

Установлено, что наилучшими экранирующими характеристиками обладают образцы из хлопчатобумажной ткани с покрытием из сплава Fe–Cr–Ni. Для этих образцов коэффициент отражения составил от –1,5 до –15,5 дБ, а коэффициент передачи — от –0,1 до –4,4 дБ.

ПРОЦЕССОР АЛГОРИТМА КРИПТОГРАФИЧЕСКОГО ХЕШИРОВАНИЯ SHA-1 НА БАЗЕ FPGA

Е.В. ЛИСТОПАД

В докладе проводится анализ возможных архитектурных решений процессора алгоритма криптографического хеширования SHA-1 на базе field-programmable gate array (FPGA) [1] для приложений, требующих высокой производительности. Поскольку

алгоритм SHA-1 имеет последовательную природу, то при аппаратной реализации возможности параллельного выполнения операций ограничены имеющимися в алгоритме зависимостями по данным. В связи с этим рассматривается реализация процессора с итеративной архитектурой [2].

Реализованный процессор принимает на вход сообщения произвольной длины (максимум 2^{64} — 1 бит) и формирует соответствующие им 160-битные хеш-значения.

Процессор состоит из двух основных модулей: интерфейсного модуля ввода, который выполняет преобразование входного сообщения в 512-битные блоки, и модуля вычислительного ядра, который выполняет главный цикл итеративной обработки каждого блока. Обработка одного 512-битного блока выполняется в 82 такта процессорного времени, при этом пропускная способность процессора достигает уровня 6.24Mbps/MHz. Процессор оснащен полностью управляемым входным интерфейсом, что позволяет пользователю запускать и останавливать поток ввода данных.

Рассмотренная реализация процессора может быть встроена в различные системы защиты информации, работающие с цифровой подписью и хеш-кодом аутентификации сообщений.

Литература

Nalini C. Iyer, Sagarika Mandal, Implementation of Secure Hash Algorithm-1 using FPGA // Dept. of Electronics and Communication Engineering, 2013. P. 757–764.

Murat Askar, Tugba Siltu Celebi, Design and FPGA Implementation of Hash Processor // ISC Turkey, 2007. P. 85–89.

МОДЕЛИРОВАНИЕ ШУМОВЫХ ХАРАКТЕРИСТИК GaAs ТРАНЗИСТОРОВ ДИАПАЗОНА КВЧ

В.Н. МИЩЕНКО

Исследование шумовых характеристик GaAs транзисторов вызывает особый интерес, который связан с возможностью создания на основе этих приборов приемников, радиометров и ряда других устройств диапазона КВЧ. Разработана программа моделирования переноса электронов в приборах на основе полупроводниковых соединений группы A^3B^5, в которой использована процедура метода Монте–Карло при решении уравнения Пуассона для сетки 100×100 узлов. Анализ процессов переноса носителей заряда в рамках процедуры метода Монте–Карло позволяет определить значения их скорости, энергии и других параметров. При моделировании к затвору прикладывался внешний гармонический сигнал с изменяемой амплитудой и частотой 100 ГГц. Выполнив анализ Фурье для токов, протекающих через сток и затвор транзистора, определялись значения коэффициента шума, шумовой температуры и предельной чувствительности. Для полупроводниковой GaAs структуры с длиной затвора 30 нм, используемой в качестве радиометра при температуре 300 К, получено значение величины предельной чувствительности, которая равняется приблизительно $2{,}24 \cdot 10^{-13}$ Вт/$(\text{Гц})^{1/2}$. Это позволяет говорить об улучшении этого параметра по сравнению с конструкциями радиометров, использующие обычные диоды с барьером Шоттки. Выработаны рекомендации по созданию новых приборов с улучшенными шумовыми параметрами в диапазоне КВЧ. Использование исследованных структур позволяет создавать транзисторы, которые можно применить при разработке высокочувствительных приемных устройств диапазона КВЧ.