

температурах, поскольку делает возможной седиментацию порошкового компонента. Присутствие в составе гидрогеля КСl стабилизирует его структуру, обеспечивая необратимое гелеобразование — при нагревании гель больше не переходит в жидкое состояние. Это обстоятельство позволяет создавать экраны ЭМИ на основе гидрогеля ПВС с добавлением КСl, работоспособные вплоть до температур начала перехода остальных полимеров, входящих в состав материалов, в вязкотекучее состояние. Такие экраны способны без ухудшения эксплуатационных характеристик либо функционировать при повышенных температурах, либо поглощать ЭМИ более высокой мощности, чем сформированные без добавки сильного электролита.

Литература

1. Сравнение характеристик двухслойных гибких экранов электромагнитного излучения с добавками шунгита и активированного угля в отражающем слое / Н.В. Насонова [и др.] // Технические средства защиты информации: тез. докл. IX Белорус.-рос. науч.-техн. конф., Минск, 28–29 июня 2011 г. – Минск: БГУИР, 2011. – 100 с. – С. 71–72.

РЕАЛИЗАЦИИ ПРОЦЕССОРОВ АЛГОРИТМА SHA-1 НА БАЗЕ FPGA

Е.В. Листопад, М.В. Качинский, А.В. Станкевич

Алгоритм SHA-1 используется в криптографических приложениях и протоколах для вычисления хэша от входного сообщения. Для использования алгоритма в вычислительных системах требуются его реализации в виде встраиваемых процессоров. В докладе рассматриваются следующие архитектуры процессоров: полностью итеративная архитектура, конвейерная архитектура на уровне раунда (шага алгоритма), полностью конвейерная архитектура.

В полностью итеративной архитектуре используется один вычислительный блок, реализующий шаг алгоритма за один такт процессора. Данные для каждого шага на вход вычислительного блока подаются в цикле. Такая архитектура обеспечивает минимальное использование ресурсов FPGA и минимальное быстродействие процессора.

В конвейерной архитектуре на уровне раунда также используется один универсальный вычислительный блок. Возможны два варианта его реализации: с использованием двухступенчатой и четырехступенчатой конвейерной архитектуры. Первый вариант предполагает вычисление шага за два такта, второй – за четыре. Такая архитектура позволяет повысить тактовую частоту и при этом не требует существенных дополнительных ресурсов FPGA по сравнению с полностью итеративной архитектурой.

В полностью конвейерной архитектуре используется по одному вычислительному блоку для каждого шага алгоритма. В такой реализации процессор одновременно вычисляет хэш-значения 80 входных сообщений, при этом первое значение получается через 82 такта, а последующие – каждый такт. Такая архитектура обеспечивает самую высокую скорость вычисления хэша, однако, требует максимального использования ресурсов FPGA по сравнению с другими рассмотренными вариантами.

НИТРИД ГАЛЛИЯ – ПЕРСПЕКТИВНЫЙ МАТЕРИАЛ РАДИАЦИОННО-СТОЙКИХ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ

И.Ю. Ловшенко, В.Р. Стемпицкий

Новыми перспективными приборами с широким спектром практических применений являются структуры на основе полупроводниковых нитридов. Высокая термическая, химическая и радиационная стойкость нитрида галлия (GaN) позволяет использовать его для изготовления приборов, работающих при повышенных температурах и в неблагоприятных условиях. Высокая теплопроводность упрощает решение проблем охлаждения рабочей области, а сочетание высокой подвижности электронов и значительного поля пробоя делает его пригодным для изготовления мощных высокочастотных и высокотемпературных транзисторов [1].