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.