УДК

МОДИФИЦИРОВАННЫЙ УМНОЖИТЕЛЬ КАРАЦУБЫ ДЛЯ УСТРОЙСТВА РЕШЕНИЯ УРАВНЕНИЙ В КОДЕ РИДА-СОЛОМОНА

САМАНТА ДЖ.[1], БХАУМИК ДЖ.[1], БАРМАН С.[2]

[1]*Халдийский технологический институт, Индия, Халдия, West Bengal*
[2]*Калькуттский университет, Индия, Калькутта, Западная Бенгалия*

Аннотация. Арифметики конечных полей широко используются в линейных блочных кодах, таких как код БЧХ и код Рида-Соломона, а также в криптографических алгоритмах. Умножители конечных полей играют важную роль и занимают значительную часть площади в конструкции СБИС. В этой работе представлен улучшенный обобщенный умножитель Карацубы. Оптимизация алгоритма умножения Карацубы осуществлена путем разделения сомножителей на две альтернативные формы, и выражения всех членов с помощью повторяющейся процедуры. Выполнено сравнение аппаратных требований предложенного умножителя со стандартным умножителем Карацубы. Предложенный умножитель требует меньшего количества сложений по сравнению с традиционным и общая площадь сокращается на 53,75% (без редукции) и на 52,08% (с редукцией). Кроме того, предложенный умножитель обладает быстродействием на 3,63% (без редукции) и 3,91% (с редукцией) выше, чем у традиционного умножителя Карацубы. Предложенный модифицированный умножитель Карацубы использован для расчета ключевого уравнения в декодере RS(47, 41), который находит применение в интеллектуальных домашних сетях. Все работы по моделированию выполнены с использованием моделирующей системы Xilinx 14.3 ISE и реализованы на семействе устройств Vertex 5 FPGA.

Ключевые слова: конечные поля; алгоритм Карацубы; умножитель полей Галуа; решающее устройство уравнения; код Рида-Соломона; СБИС; ПЛИС; программируемая логическая интегральная схема

1. ВСТУПЛЕНИЕ

Алгоритм Карацубы (АК) представляет собой быстродействующий алгоритм умножения, имеющий широкий диапазон применения в области кодов с исправлением ошибок, криптографических алгоритмов, генерации псевдослучайных чисел и обработки сигналов. Суммирование конечных полей может быть реализовано на малой площади, тогда как умножение требует большой площади кристалла.

Умножители конечных полей возможно разделить на три категории: битово-последовательный умножитель [1], битово-параллельный умножитель [2] и гибридный умножитель. Битово-параллельные структуры являются более быстродействующими и используют только комбинационные логические элементы [3], тогда как битово-последовательные структуры требуют меньше площади и используют регистры, помимо комбинаторных логических схем [1]. Гибридные умножители частично битово-последовательные и частично битово-параллельные; в результате, они более быстродействующие, чем битово-последовательные, и занимают меньшую площадь, чем битово-параллельные.

Электронный вариант статьи: http://radio.kpi.ua/article/view/S0021347015100039