К ВЫБОРУ СТРУКТУР СУММАТОРОВ ДЛЯ АРИФМЕТИЧЕСКИХ БЛОКОВ В УСТРОЙСТВАХ ТЕОРЕТИКО-ЧИСЛОВОГО ПРЕОБРАЗОВАНИЯ

Лунин Д.А., Дегтярев В.О.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

В настоящее время широкое распространение получили так называемые теоретико-числовые преобразования (ТЧП), у которых промежуточные результаты вычислений принимают только квантованные (целые) значения. Эти преобразования обладают свойством свертки и могут найти применение для фильтрации и сжатия сигналов и изображений.

Применение на практике таких преобразований во многих случаях ограничено в связи с большим требуемым объемом вычислений. В то же время существует ряд так называемых быстрых алгоритмов, позволяющих вычислять коэффициенты преобразования существенно проще.

Для вычисления ТЧП необходимо устройство управления и арифметико-логическое устройство (АЛУ). Устройство управления генерирует адреса, подаваемые на ОЗУ и ПЗУ из которых считываются входные данные и элементы матрицы преобразования соответственно. Далее эти значения отправляются на АЛУ, после чего данные хранятся в ОЗУ до очередного этапа вычисления «бабочки».

АЛУ содержит два основных элемента: сумматор и умножитель по модулю p. Однако сумматоры по модулю p также используются в качестве последнего этапа при суммировании в умножителях по модулю p. Поэтому необходимо ускорить операцию сложения, а именно время вычисления переноса должно быть минимизировано. Одним из решений является использование сумматоров с ускоренным переносом. Было выявлено, что ПЛИС реализация сумматоров с ускоренным переносом по модулю 2^n+1 в коде «diminished-1» наиболее подходяще для представления элементов конечного поля $GF(p)$.

Рассмотрены структурные схемы для сумматоров по модулю 2^n+1 работающие в коде «diminished-1». Это параллельно-префиксные сумматоры со структурами переноса префикса Ладнер-Фишер и Когге-Стоуна.

Моделирование на ПЛИС показало, что структуры сумматоров с ускоренным переносом по модулю 2^n+1 в коде «diminished-1» приводят к более эффективной реализации в отношении таких параметров, как *вентильное пространство* и *время выполнения операции.* Также моделирование выявило различие между структурами переноса префикса Ладнер-Фишер и Когге-Стоуна. Структура Ладнер-Фишер работает медленнее, но содержит меньше логических элементов, чем структура Когге-Стоуна.