СТРУКТУРЫ УМНОЖИТЕЛЕЙ, ПОСТРОЕННЫЕ С ПРИМЕНЕНИЕМ ТЕОРЕТИКО-ЧИСЛОВЫХ ПРЕОБРАЗОВАНИЙ

Лунин Д.А.

Национальный технический университет «Харьковский политехнический институт», г. Харьков

Умножители по модулю используются в различных приложениях, например для систем счисления остаточных классов (СОК), отказоустойчивых компьютерных систем и криптографии.

Теоретико-числовое преобразование (ТЧП), выполненное в СОК, у которых промежуточные результаты вычислений принимают только квантованные (целые) значения, обладают свойством свертки и могут найти применение для фильтрации и сжатия сигналов и изображений.

Применение на практике СОК ограничено, в связи с большим требуемым объемом вычислений. В то же время существует ряд так называемых быстрых структур для вычисления умножения, которые позволяют вычислить конечный результат существенно проще.

В частности, арифметика по модулю $(2^n + 1)$ находится в центре внимания многих исследовательских работ, потому что этот модуль является частью хорошо известного тройного набора модулей $\{2^n-1, 2^n, 2^n +1\}$, который широко используется для общей и специальной формы представления СОК. Модель компонентов модуля $(2^n + 1)$, кажется более перспективной из этого тройного набора модулей, так как компоненты модуля $(2^n + 1)$ работают с операндами более широкой размерности в сравнении с двоичными каналами, но при этом возникают трудности в реализации. Для решения этой проблемы, Лейбовиц ввел кодирование "diminished-1". В соответствии с этим кодированием каждое число представлено с уменьшением на 1, а операнд нуль представлен с использованием отдельного бита индикации. Это представление имеет преимущество в том, что числа представлены n битами. Это существенно упрощает основные операции, такие как сложение, умножение и округление по модуля $(2^n + 1)$.

Предлагаемая структура умножителя предполагает, что множитель или множимое не равны нулю, то есть нуль должен быть исключен до подачи значений на вход умножителя. Используя параллельную модульную структуру умножителя по модулю $(2^n + 1)$ основанную на дереве Уоллеса можно получить регулярные структуры и следовательно реализация структур умножителей больших разрядностей на СБИС упрощается.

Моделирование на ПЛИС показало, что промежуточные структуры позволяют добиться компромиссов между количеством внутренних соединений и разветвления промежуточных узлов, и таким образом достигается более эффективное соотношение, между скоростью вычисления и вентильной емкостью ПЛИС, по сравнению с любым из известных конечных случаев.