МЕТОДЫ СИНТЕЗА УМНОЖИТЕЛЕЙ МОНТГОМЕРИ, ОПЕРИРУЮЩИХ В КОНЕЧНЫХ ПОЛЯХ

Поваляева А.Н.

Национальный технический университет «Харьковский политехнический институт, г. Харьков

В данной работе рассмотрены вопросы одного из ключевых инструментов защиты информационных систем – криптографии. Ее сущность заключается в использовании преобразований информации, доступных законным сторонам информационного цикла и недоступных всем остальным. В настоящее время для защиты информации находят широкое применение криптопроцессоры. Одной из составных частей криптопроцессора является арифметико-логическое устройство, которое производит криптопреобразование в зависимости от применяемого криптоалгоритма. Операции в криптоалгоритмах выполняются над элементами конечных полей.

Среди арифметических операций, проводимых над конечными полями, наиболее важными являются операции умножения и возведения в квадрат. Обычно приходится выполнять умножение целых рациональных чисел по простому или составному модулю или умножение полиномов по модулю неприводимого полинома. Если выполнять модульное умножение непосредственно, сначала перемножая целые числа (полиномы), а затем, вычисляя остаток от деления, то сложность алгоритма будет определяться процедурой нахождения остатка. Монтгомери был предложен метод модульного умножения, не требующий выполнения операции деления.
Этот метод позволяет выполнять быстрое умножения чисел большой разрядности по модулю простых чисел.

В настоящее время разработчиками используются три основных метода построения умножителей Монтгомери и соответствующие им архитектуры: разрядно-последовательная, пословно-последовательная и параллельная.

Для разрядно-последовательного умножения рассматриваются два алгоритма: алгоритм умножения со старшим значащим битом (СЗБ) и алгоритм умножения с младшим значащим битом (МЗБ).

В данной работе был предложен метод синтеза умножителей Монтгомери в полях Галуа с разрядно - последовательной и параллельной архитектурой. На основе рассмотренных методов разработан алгоритм синтеза умножителей. Также разработаны компьютерные модели синтезированных умножителей в среде Active-HDL.