30. Simulation of synthetic aperture radar imaging of dynamic wakes of submerged body / Peng Liu, Ya-Qiu Jin // Journals & Magazines: IET Radar, Sonar & Navigation. Volume: 11, Issue: 3. – P. 481 – 489. – URL: https://ieeexplore.ieee.org/document/7887099. -- Дата публикации: 24.04.2017.

31. Tunaley J.K.E. The Bernoulli Hump Generated by a Submarine. – URL: http://www.london-research-and-development.com/Bernoulli-Hump.pdf. – Дата обращения 01.03.2015.

Подтверждаю согласие на опубликование статьи в Интернете (в системе РИНЦ или на сайте издания).

Автор: 09 июня 2019 г. В. Поленин

МОДЕЛИРОВАНИЕ ФОРМИРОВАТЕЛЯ ЧАСТИЧНЫХ ОСТАТКОВ УСТРОЙСТВА ПРИВЕДЕНИЯ ПО МОДУЛЮ

***Әділбеккызы Сайран*[1]**
***Айтхожаева Евгения Жамалхановна*[2]**
***Тынымбаев Сахыбай*[3]**
[1]Магистр военного дела и безопасности, инженер
[2]Канд. техн. наук, ведущий научный сотрудник
[3]Канд. техн. наук, научный руководитель проекта
Алматинский Университет Энергетики и Связи, г.Алматы, Казахстан
DOI: 10.31618/ESU.2413-9335.2019.2.63.167

АННОТАЦИЯ

Разрабатывается структура быстродействующего устройства приведения по модулю с оптимальными аппаратными затратами. Выполняется разработка принципиальной схемы устройства в САПР Quartus Prime Lite Edition. Приводятся результаты моделирования формирователя частичных остатков - основного блока устройства приведения по модулю. Временное моделирование устройства подтверждает его высокое быстродействие: F_{MAX}*=68,77МГц*.

ABSTRACT

A structure for a high-speed modular reduction device, which has optimal hardware costs, is being developed. The schematic diagram of the device is implemented in CAD Quartus Prime Lite Edition. The simulation results of the partial remainder former that is the main unit of the device for modular reduction, are presented. The time modeling of the device confirms its speed: F_{MAX} = 68.77 MHz.

Ключевые слова: асимметричный криптоалгоритм, приведение по модулю, моделирование.

Keywords: asymmetric cryptoalgorithm, modular reduction, simulation.

Введение. Аппаратное шифрование имеет ряд существенных преимуществ перед программным шифрованием, одним из которых является более высокое быстродействие. Проектирование и реализация оптимальных схемных решений одной из базовых операций асимметричного криптоалгоритма RSA – приведения чисел по модулю, является актуальной задачей в связи с широким применением на практике данного алгоритма и его низким быстродействием по сравнению с симметричными алгоритмами. Последнее обстоятельство сдерживает применение асимметричных криптосистем, несмотря на такое их преимущество, как отсутствие необходимости распространения секретных ключей, что является недостатком симметричных криптосистем.

Приведение по модулю является наиболее затратной операцией по времени по сравнению с другими используемыми операциями в алгоритме RSA, чем и объясняется повышенный интерес к созданию быстродействующих устройств приведения по модулю.

Основная часть. Имеется большое количество публикаций, в том числе и патентов, в которых предлагаются различные алгоритмы и устройства приведения по модулю [1-4]. Большинство предлагаемых решений является неприемлемыми при реализации алгоритма RSA, так как при его реализации необходимо выполнять сложные и громоздкие математические вычисления над очень большими (многоразрядными) числами, что приводит к большим аппаратным затратам. В [5] был предложен метод на основе модификации и адаптации машинного деления двоичных чисел и разработана структурно-функциональная схема нового быстродействующего устройства приведения *2n*-разрядного числа *A* по *n*-разрядному модулю *P* (*R=A mod P*) с оптимальными аппаратными затратами. Повышение быстродействия устройства достигается путем сдвига остатков на два разряда влево для уменьшения тактов выполнения операции приведения по модулю. На рисунке 1 приведена структура данного устройства с выделением основных составляющих блоков.

На управляющий блок поступают сигналы *Сброс*, *Пуск*, тактовые импульсы (*ТИ*), *K=n/2* (*n* – разрядность модуля *P*, *n/2* - определяет число тактов, необходимых для выполнения операции приведения по модулю).

В блоке формирователя кратных модуля *P* предварительно вычисляются прямые и обратные (для выполнения в дальнейшем операции вычитания) коды удвоенного и утроенного модуля (*2p и 3p*).

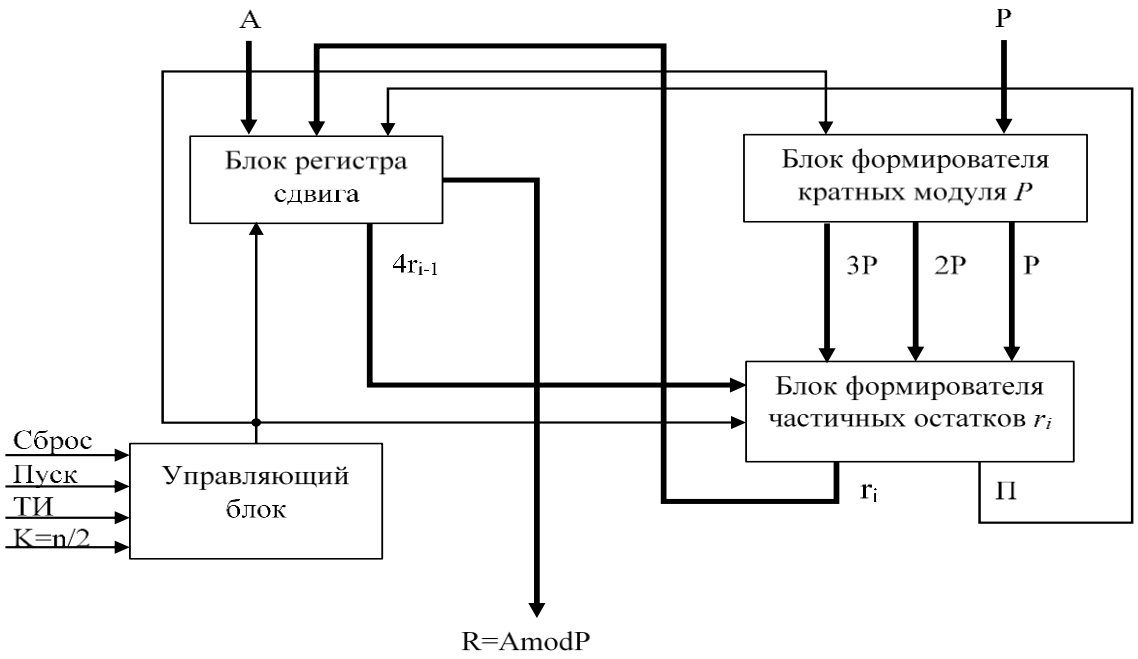

Рисунок 1. Структура устройства быстрого приведения чисел по модулю

Затем, в блоке формирователя частичных остатков (ФЧО), в первом такте определяются старшие разряды частичного остатка путем вычитания в дополнительном коде *p* или сформированных кратных модуля (*2p* или *3p*) из сдвинутого на два разряда вправо приводимого числа *A*, т.е. увеличенного в 4 раза. Используются (*n+2*) старших разрядов (обозначено далее $4r_0$) сдвинутого на два разряда вправо *2n*-разрядного числа A, которые подаются на ФЧО.

В состав ФЧО входят сумматор, логические элементы *И* и *ИЛИ*, мультиплексор и три схемы сравнения, которые используются для определения операции, которую необходимо выполнить на сумматоре, чтобы определить значение старших разрядов очередного остатка (r_i): вычитание *p*, или *2p*, или *3p*.

Полученный очередной остаток r_i, при наличии сигнала переноса *П* =1 из старшего разряда сумматора, записывается в старшие разряды регистра сдвига *A* (блок регистра сдвига). И в последующих тактах вычитание *p*, или *2p*, или *3p* выполняется из (*n+2*) старших разрядов сдвинутого на два разряда имеющегося числа в регистре сдвига *A* (полученного частичного остатка r_i и следующих двух разрядов).

Пример работы устройства.

Пусть *n=6, 2n=12, n+2=8, n/2=3.*

Приводимое число $A=638_{10}=001001111110_2$ записывается в блоке регистра сдвига в $РгА=00.001001111110_2$. Здесь, и в дальнейшем, точкой отделены 2 старших дополнительных разряда.

Значение модуля $P=35_{10}=100011_2$ записывается в блоке формирователя кратных модуля *P* в *РгР* в прямом коде $[p]_{пр}=00.100011_2$. В этом же блоке формируются кратные модуля *P*: $[2p]_{пр}=01.000110_2=70_{10}$, $[3p]_{пр}=01.101001_2=105_{10}$. Здесь для обозначения прямого кода модуля *p* используется обозначение $[p]_{пр}$, обратного кода модуля используется обозначение $[p]_{обр}$, а для обозначения дополнительного кода используется обозначение $[p]_{доп}$. При $P=35_{10}=100011_2$: $[p]_{обр}=11.011100_2$, $[2p]_{обр}=10.111001_2$, $[3p]_{обр}=10.010110_2$, $[p]_{доп}=11.011101_2$, $[2p]_{доп}=10.111010_2$, $[3p]_{доп}=10.010111_2$.

Вычисления по определению остатка *R=A mod P* приведены для наглядности в двоичной и десятичной системах счисления в таблице 1, в которой старшие разряды частичных остатков, получаемые в ФЧО, обозначены через r_i . Нумерация разрядов регистров выполняется справа налево, начиная с нуля.

Для определения правильности работы устройства было выполнено моделирование разработанного устройства приведения по модулю. В качестве среды для проектирования и отладки проекта был использован программный продукт фирмы Altera – САПР Quartus Prime Lite Edition, который позволяет построить принципиальную и поведенческую модели устройства и проверить его работоспособность с иллюстрацией на временных диаграммах, а также получить временные характеристики моделируемого устройства. Среда проектирования позволяет запустить функциональное и временное моделирование. Функциональное моделирование проекта позволяет проверить правильность работы цифрового устройства с точки зрения логики и схемотехники. Временное моделирование проекта позволяет проверить не только правильность логического функционирования, но и работу с учетом задержки распространения сигналов в реальной программируемой логической интегральной схеме.

Таблица 1.

Порядок вычисления *R = A mod P*

Тактовые импульсы	Выполняемые операции
ТИ1	$4r_0=00.100111_2=39_{10}$ (после сдвига влево на 2 разряда старшие 8 разрядов *РгА)*. Так как $35<39<70$ $(p<4r_0<2p)$, схемами сравнения с помощью мультиплексора вырабатывается сигнал на вычитание *p*. На сумматоре в ФЧО выполняется операция: $[4r_0]_{пр} = 00.100111$ $[p]_{доп} = 11.011101$ ✚ $r_1 = 00.000100$ —————— Сигнал переноса из старшего разряда сумматора *П=1,* поэтому r_1 перезаписывается в старшие разряды $РгА(13\div6):= 00.000100_2 = 4_{10}$
ТИ2	$4r_1=00.010011_2=19_{10}$ (после сдвига влево на 2 разряда старшие 8 разрядов *РгА)*. Так как $4r_1<p$, схемами сравнения не вырабатывается сигнал на вычитание. Сигнал переноса *П=0,* поэтому $РгА(13\div6):= 00.010011_2 = 19_{10}$ остается без изменения.
ТИ3	$4r_2=01.001110_2=78_{10}$ (после сдвига влево на 2 разряда старшие 8 разрядов *РгА)*. Так как $70<78<105$ $(2p<4r_2<3p)$, схемами сравнения вырабатывается сигнал на вычитание $2p$. На сумматоре ФЧО выполняется операция: $[4r_2]_{пр} = 01.001110$ $[2p]_{доп} = 10.111010$ ✚ $r_3 = 00.0001000$ —————— Сигнал переноса из старшего разряда сумматора *П=1*, поэтому r_3 перезаписывается в старшие разряды $РгА(13\div6):=00.001000_2 = 8_{10}$. Конечный результат $R=00.001000_2 = 8_{10}$ Проверка: $R = 638 - \left]\frac{638}{35}\right[35 = 8_{10} = 1000_2$

Проектирование устройства было выполнено с ориентацией на низкобюджетную плату DE0-CV с программируемой логической интегральной схемой FPGA семейства Cyclone VE base, выпускаемой фирмой Altera – 5CEBA4F23C7.

Разработка принципиальной схемы устройства выполнялась поэтапно по блокам с проверкой их работы для разрядности *n=6*. Ниже показана реализация основного блока ФЧО, для которого первоначально были спроектированы его составляющие: сумматор, мультиплексор и три схемы сравнения. А также были использованы логические элементы *И* и *ИЛИ*.

Для реализации схем сравнения были использованы интегральные схемы серии 7400, включенные в библиотеку Altera Quartus Prime '/others/maxplus2/' – 7485 (4-битный компаратор). Графический файл 8-разрядной схемы сравнения показан на рисунке 2.

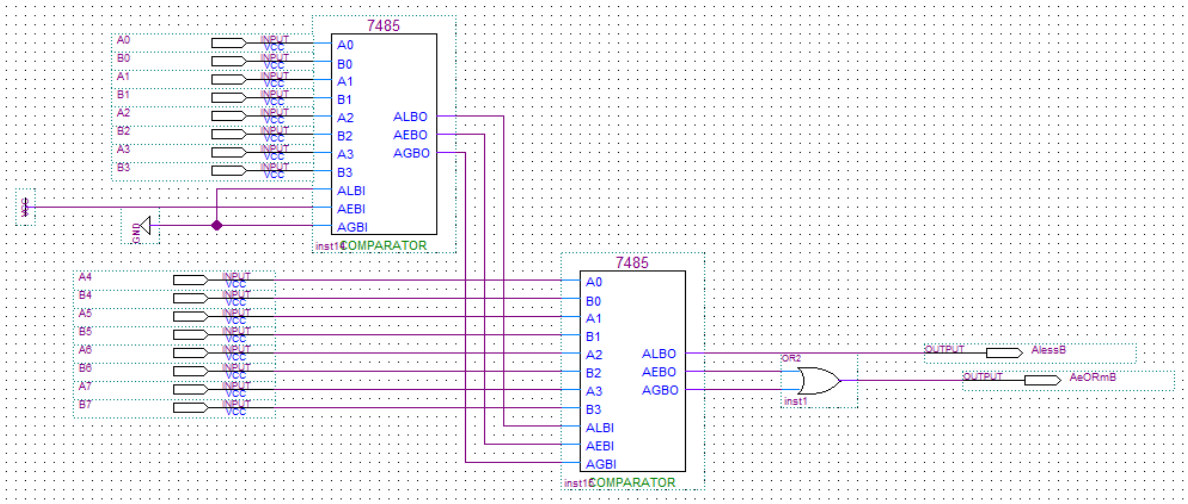

Рисунок 2. Схема 8-разрядного компаратора (схемы сравнения)

Для создания сумматора был использован 4-битный сумматор – 74283 из серии интегральных схем 7400, включенных в библиотеку Altera Quartus II '/others/maxplus2/'. Графический файл 8-разрядного сумматора показан на рисунке 3. Были также спроектированы и другие компоненты ФЧО.

Были получены символ-модули разработанных компонентов ФЧО и с их использованием был собран блок ФЧО (*FPR*), принципиальная схема которого представлена на рисунке 4. В принципиальной схеме ФЧО были использованы:

символ модуля регистра *РгР* (1), символ мо-

дуля сумматора для получения *3p* (2), символ модуля блока логических элементов *И* для подачи на вычитающий сумматор старших восьми разрядов из *РгА* (3), символ модуля схемы сравнения сдвинутого полученного остатка с *p* (4), символ модуля схемы сравнения сдвинутого полученного остатка с *2p* (5), символ модуля схемы сравнения сдвинутого полученного остатка с *3p* (6), символ модуля мультиплексора для подачи на вычитающий сумматор *p* или *2p* или *3p* (10), символ модуля вычитающего сумматора определения старших разрядов частичного остатка - r_i (11). Логические элементы *И* (7,8) и логический элемент *ИЛИ* (9) используют результаты схем сравнения и служат для выработки управляющих сигналов, подаваемых на мультиплексор (10), которые определяют подачу на вычитающий сумматор или *p*, или *2p*, или *3p*.

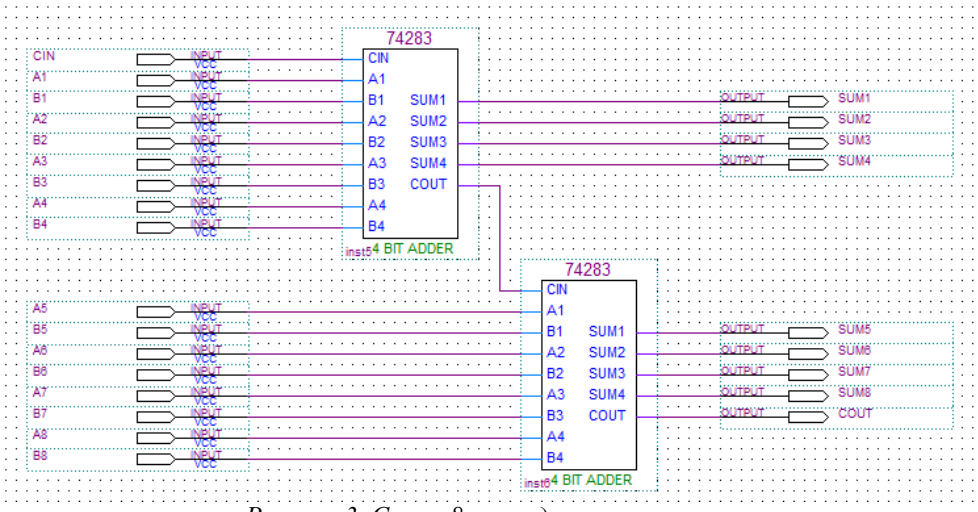

Рисунок 3. Схема 8-разрядного сумматора

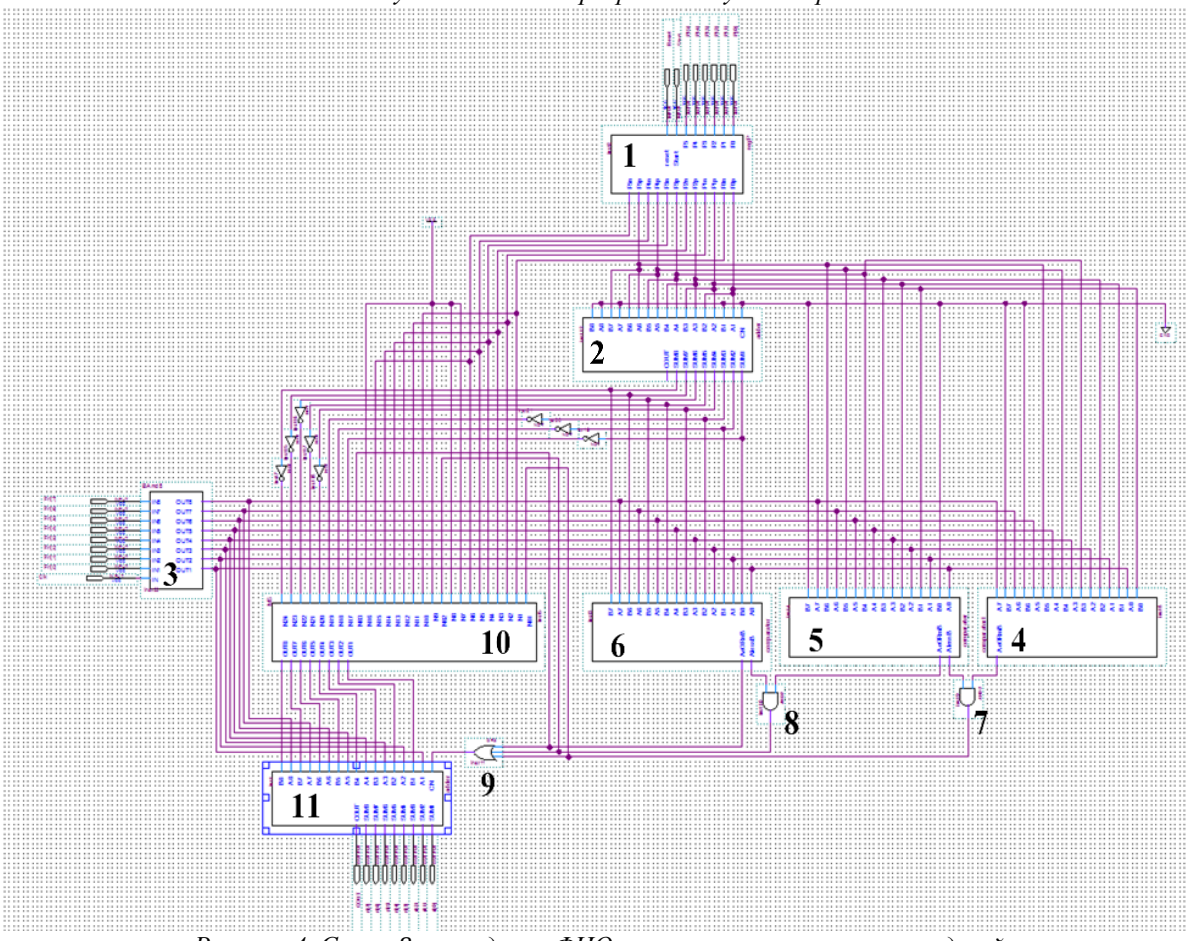

Рисунок 4. Схема 8-разрядного ФЧО с использованием символ-модулей

Были получены временные диаграммы работы ФЧО, фрагмент которых приведен на рисунке 5.

В качестве входных данных были использованы параметры из примера, приведенного в таблице 1: $P=35_{10}=100011_2$, $4r_0=39_{10}=00.1000111_2$. Как видно на временной диаграмме, результат сложения в вычитающем сумматоре ($r_1=4_{10}=00.00000100_2$) соответствует значению r_1 из примера.

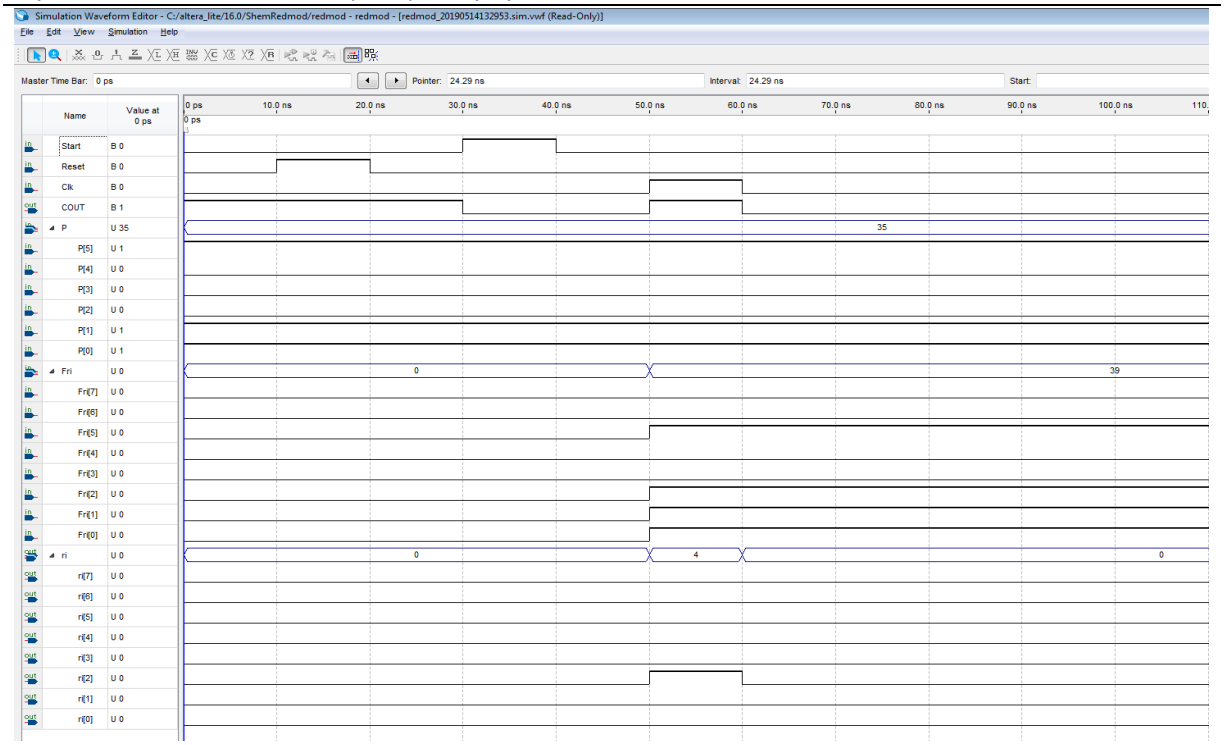

Рисунок 5. Временные диаграммы работы 8-разрядного ФЧО

Заключение. Реализация устройства приведения по модулю была выполнена полностью в Quartus Prime Lite Edition и получены его временные характеристики.

Анализ временных характеристик показал, что принципиальная модель устройства будет работать медленнее в режиме *Slow* при напряжении *1100 mV* и температуре *85℃* (модель работы в худших условиях). Максимальная тактовая частота при этом F_{MAX}*=32,91МГц*. А в нормальных условиях работы максимальная тактовая частота составляет для принципиальной модели F_{MAX}*=68,77МГц*. Тактовая частота существующих специальных процессоров RSA составляет от *5МГц* до *30МГЦ*, что намного меньше, чем тактовая частота разработанного устройства быстрого приведения чисел по модулю [6].

Список литературы:

1. Ковтун М., Ковтун В. Обзор и классификация алгоритмов деления и приведения по модулю больших целых чисел для криптографических приложений. [Электронный ресурс]. URL: https://docplayer.ru/30671408-Obzor-i-klassifikaciya-algoritmov-deleniya-i-privedeniya-po-modulyu-bol-shih-celyh-chisel-dlya-kriptograficheskih-prilozheniy.html.

2. Устройство для формирования остатка по произвольному модулю от числа: пат. 2445730 Рос. Федерация: МПК H03M 7/18, G06F 7/72 / Копытов В.В., Петренко В.И., Сидорчук А.В.; заявитель и патентообладатель ГОУ ВПО Ставропольский государственный университет. – №2010106685/08; заявл.24.02.2010; опубл.27.08.2011, Бюл. №24 – 8 с.

3. Формирователь остатка по произвольному модулю от числа: пат. 30983 Рес. Казахстан: МПК G06F 7/72 H03M 7/18 /Айтхожаева Е.Ж., Тынымбаев С.Т.; заявитель и патентообладатель РГП на ПХВ "Казахский национальный технический университет им. К.И. Сатпаева" МОН РК . - №2014/1450.1; заявл. 05.11.2014; опубл. 15.03.2016, –5 с.

4. Adilbekkyzy S., Aitkhozhayeva E., Tynymbayev S. Analysis of devices structures for modular reduction. Proc. 16th International Scientific Conference «Information Technologies and Management» Riga, - 2018. p. 97-98.

5. Tynymbayev S., Aitkhozhayeva Y. Zh., Adilbekkyzy S. High speed device for modular reduction: Bulletin of National Academy of Sciences of the Republic of Kazakhstan, №6 (2018). - Алматы: Наука, 2018. - с.147-152. ISSN: 1991-349421. DOI: 10.32014/2018.2518-1467.38.

6. Алгоритм шифрования RSA. Криптоанализ алгоритма RSA. Конспект лекций. [Электронный ресурс]. URL: https://en.ppt-online.org/97398.