

## File Structure:

team01\_lab2

| team01\_lab2\_report.pdf

|  
└─src

| MyRsa256Core.sv

| MyRsa256Wrapper.sv

|  
└─DE2\_115

| DE2\_115.qsf

| DE2\_115.sdc

| DE2\_115.sv

|  
└─pc\_python

| enc.bin

| key.bin

| python

| rs232.cpp

| rs232.py

|  
└─golden

| dec1.txt

| dec2.txt

| dec3.txt

| enc1.bin

| enc2.bin

| enc3.bin

| key.bin

| key\_ascii.txt

| rsa.py

|  
└─tb\_verilog

| PipelineCtrl.v

| PipelineTb.v

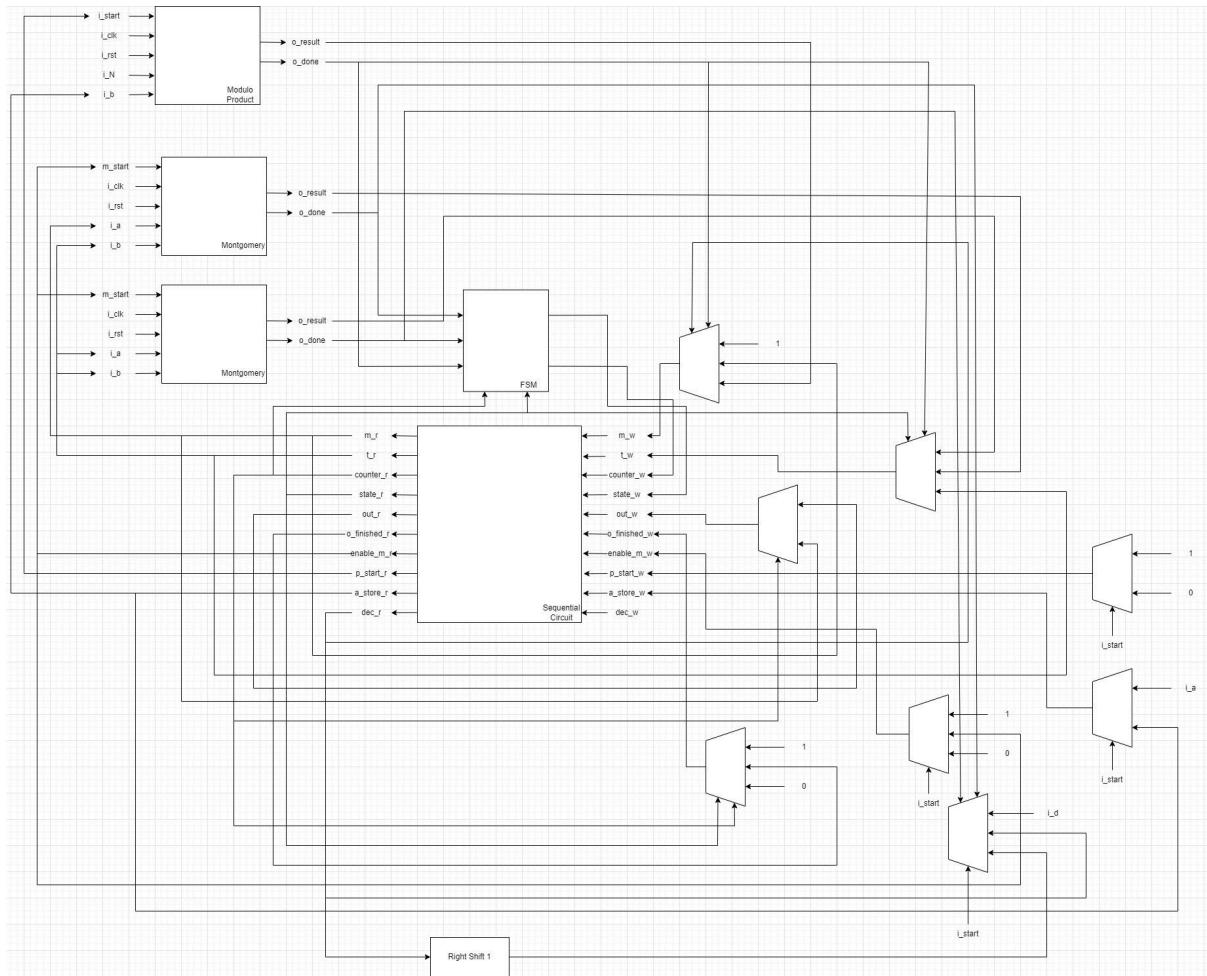
| tb.sv

| test\_wrapper.sv

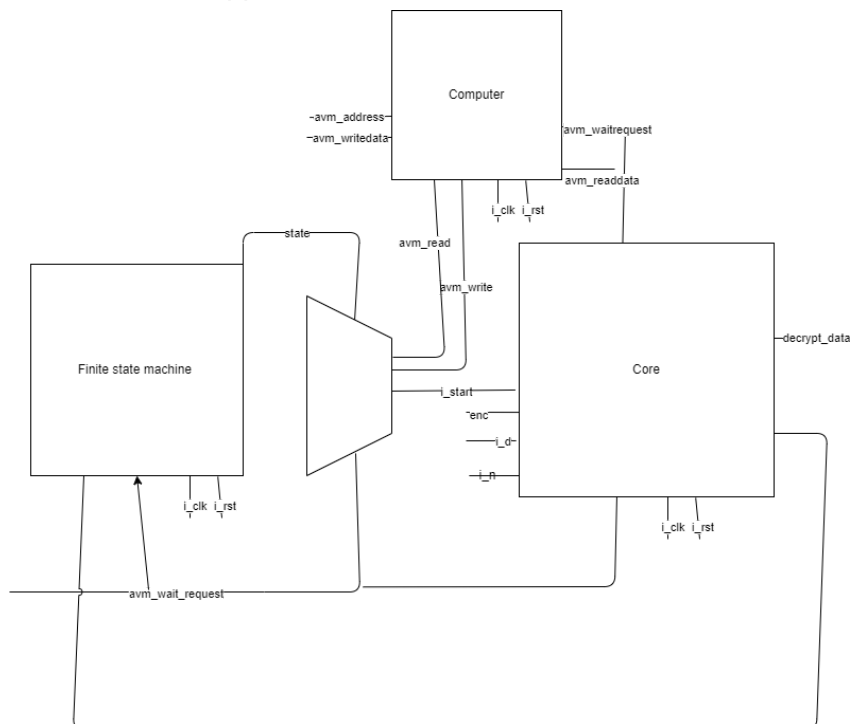
| wrapper\_input.txt

| wrapper\_output.txt

## System Architecture: Data Path of RSA\_Core:

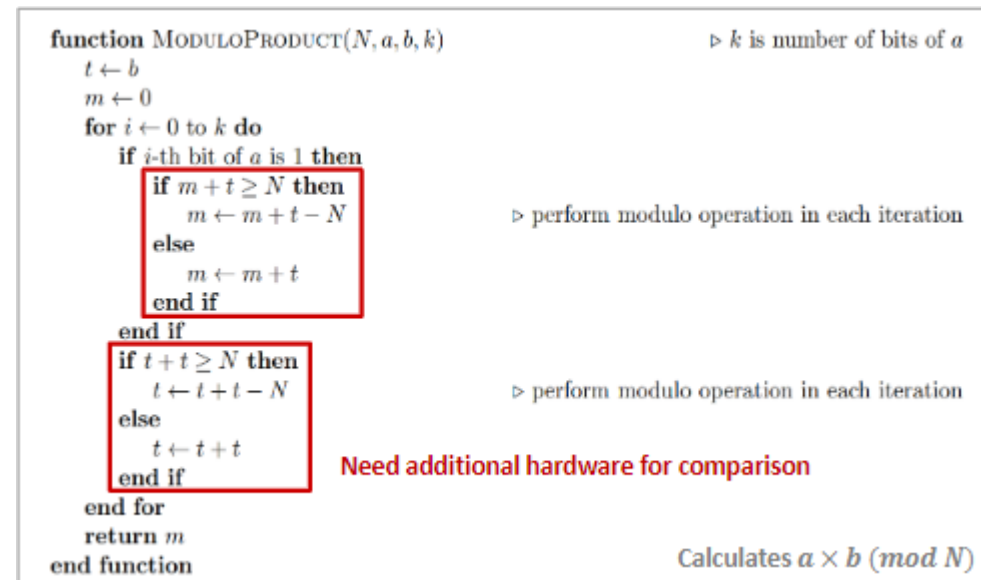


## Data Path of Wrapper:

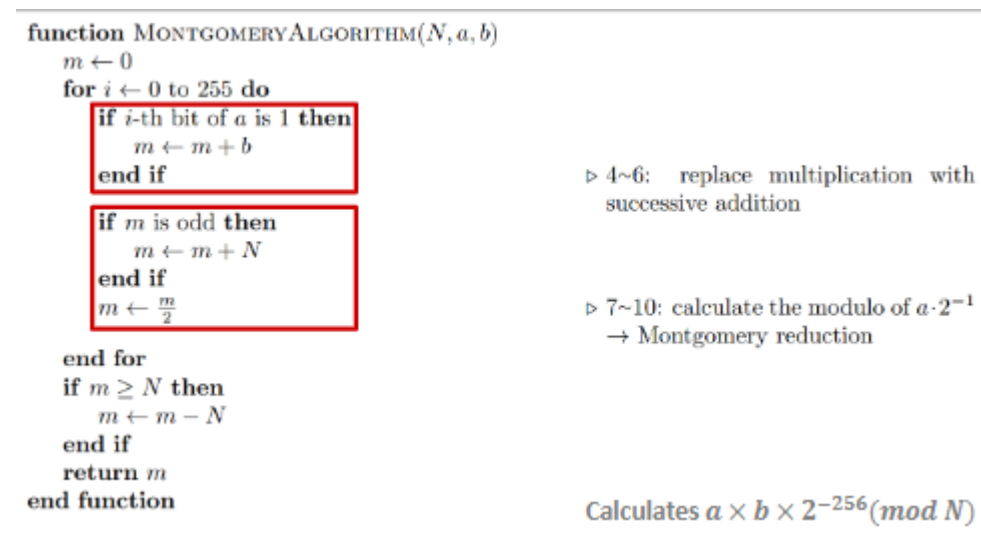


## Hardware Scheduling:

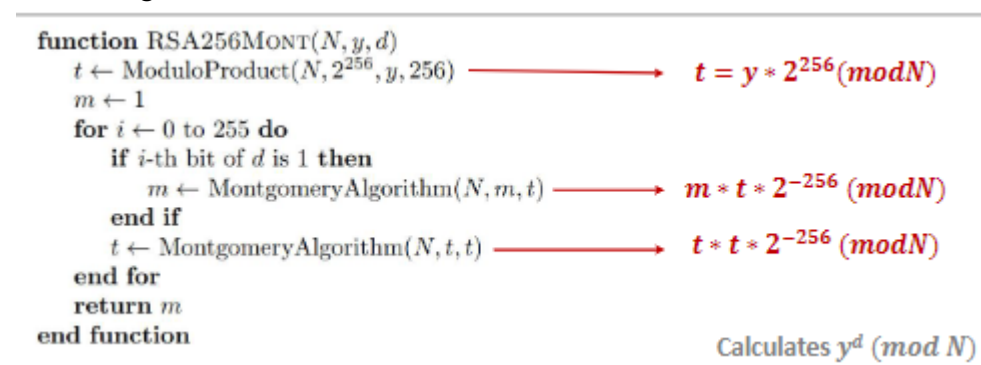
### Algorithm of Modulo Product:



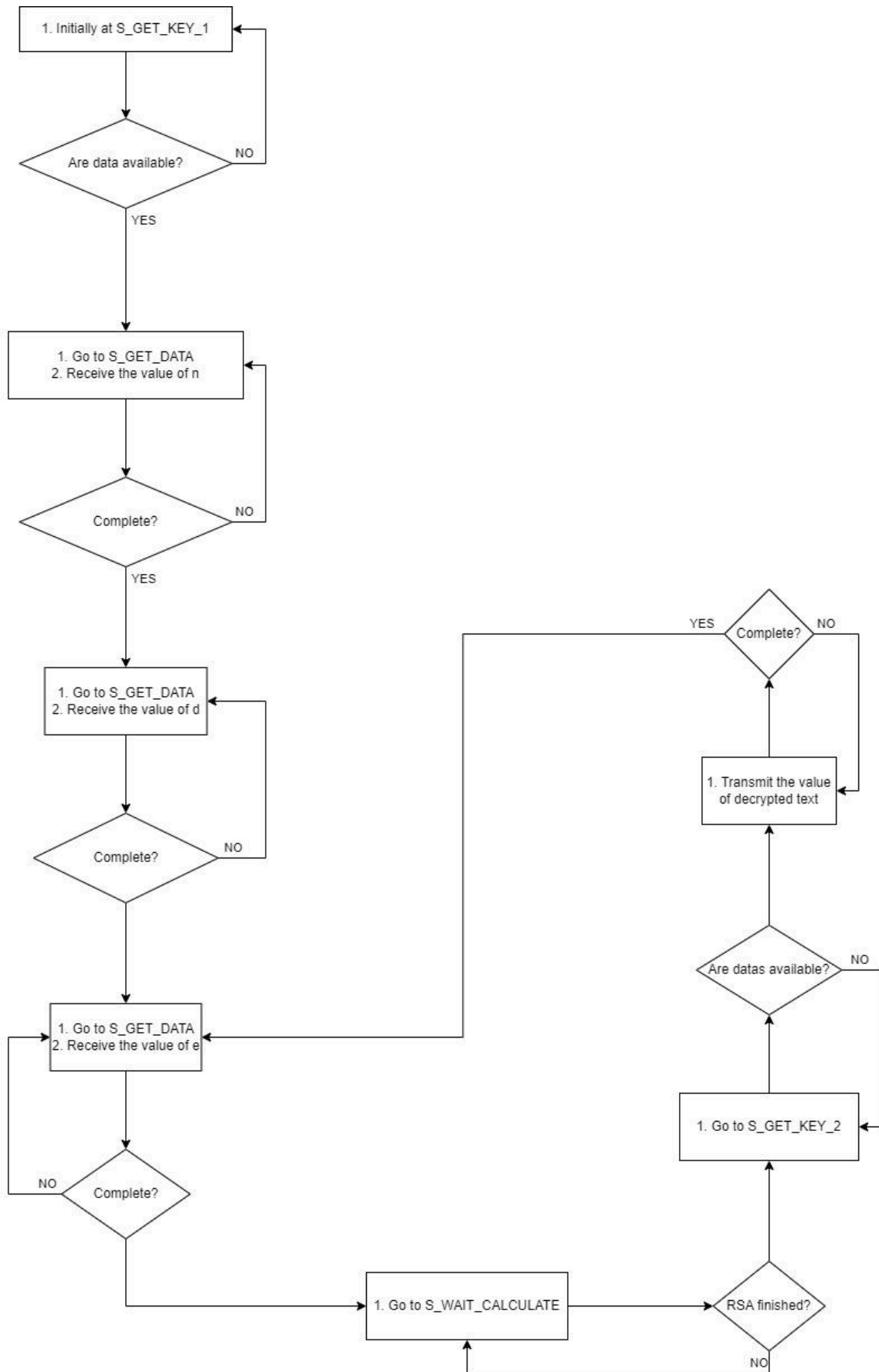
### Algorithm of Montgomery:



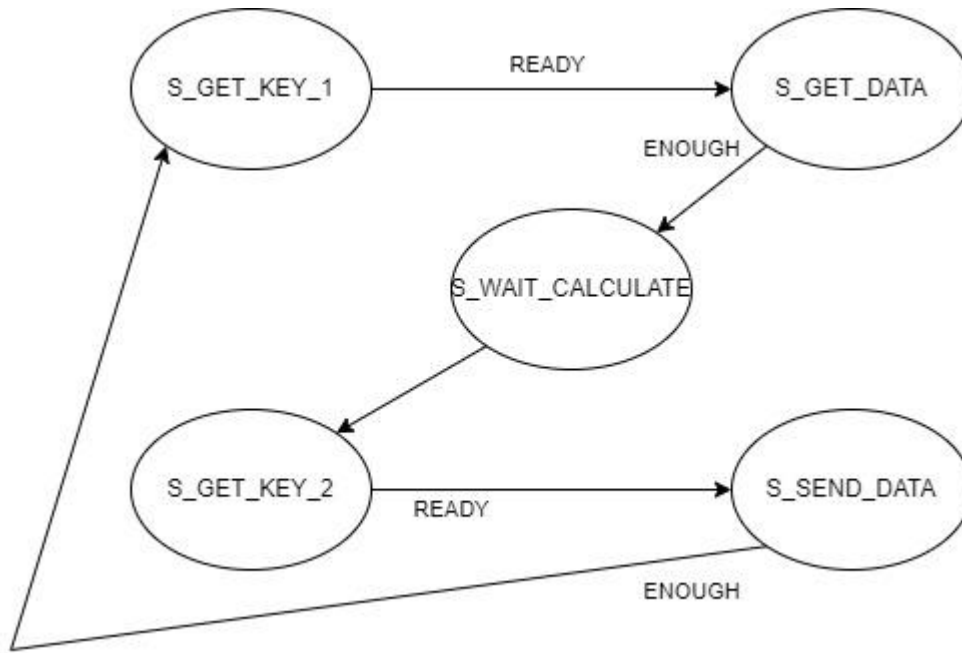
### Overall Algorithm:



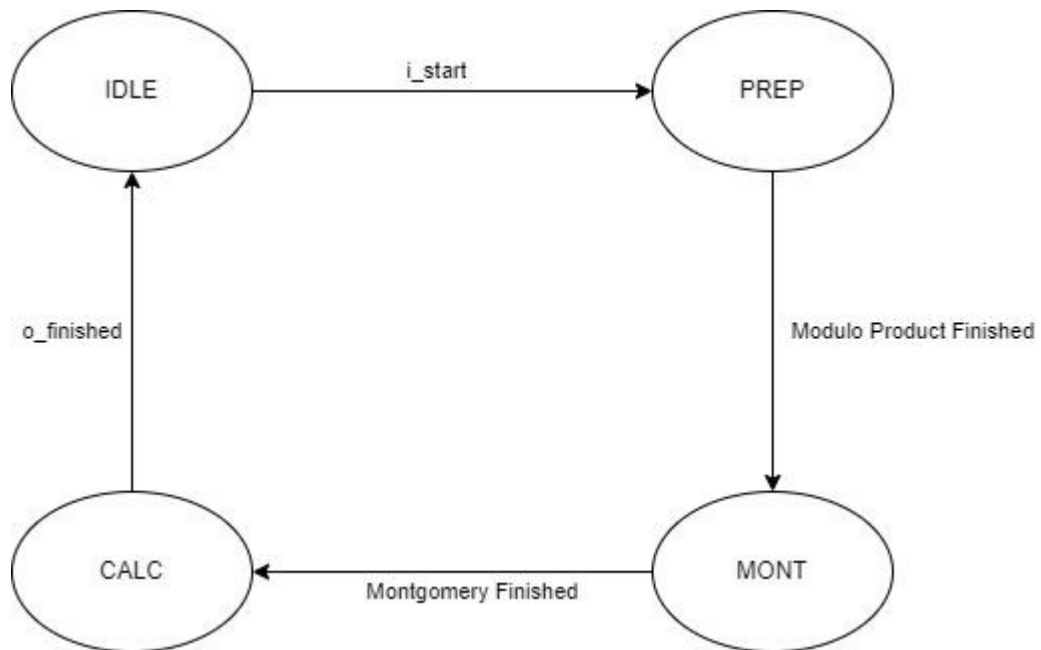
## Algorithm of Wrapper:



FSM of Wrapper:



FSM of RSA\_Core:



Fitter Summary:

DE2\_115.sv

Compilation Report - DE2\_115

MyRsa256Core.sv

MyRsa256Wrapper.sv

Table of Contents

Flow Summary

Flow Settings

Flow Non-Default Global Sett

Flow Elapsed Time

Flow OS Summary

Flow Log

Analysis & Synthesis

Fitter

Summary

Settings

Parallel Compilation

I/O Assignment Warning

Ignored Assignments

Incremental Compilation

Pin-Out File

Resource Section

I/O Rules Section

Device Options

Operating Settings and C

Messages

Suppressed Messages

Flow Messages

Flow Suppressed Messages

Assembler

TimeQuest Timing Analyzer

Summary

Parallel Compilation

SDC File List

Clocks

Slow 1200mV 85C Model

Slow 1200mV 0C Model

Fast 1200mV 0C Model

Multicorner Timing Analy

Multicorner Datasheet R

Fitter Summary

Fitter Status

Successful - Sun Mar 24 02:56:08 2024

Quartus II 64-Bit Version

15.0.0 Build 145 04/22/2015 S3 Full Version

Revision Name

DE2\_115

Top-level Entity Name

DE2\_115

Family

Cyclone IV E

Device

EP4CE115F29C7

Timing Models

Final

Total logic elements

7,956 / 114,480 ( 7 % )

Total combinational functions

6,914 / 114,480 ( 6 % )

Dedicated logic registers

3,724 / 114,480 ( 3 % )

Total registers

3724

Total pins

480 / 529 ( 91 % )

Total virtual pins

0

Total memory bits

0 / 3,981,312 ( 0 % )

Embedded Multiplier 9-bit elements

0 / 532 ( 0 % )

Total PLLs

1 / 4 ( 25 % )

Timing Analyzer:

DE2\_115.sv

Compilation Report - DE2\_115

MyRsa256Core.sv

MyRsa256Wrapper.sv

Table of Contents

Flow Summary

Flow Settings

Flow Non-Default Global Settings

Flow Elapsed Time

Flow OS Summary

Flow Log

Analysis & Synthesis

Fitter

Flow Messages

Flow Suppressed Messages

Assembler

TimeQuest Timing Analyzer

Summary

Parallel Compilation

SDC File List

Clocks

Slow 1200mV 85C Model

Slow 1200mV 0C Model

Fast 1200mV 0C Model

Multicorner Timing Analysis

Multicorner Datasheet Rep

Advanced I/O Timing

Clock Transfers

Report TCCS

Report RSKM

Unconstrained Paths

Messages

Unconstrained Paths

	Property	Setup	Hold
1	Illegal Clocks	0	0
2	Unconstrained Clocks	0	0
3	Unconstrained Input Ports	0	0
4	Unconstrained Input Port Paths	0	0
5	Unconstrained Output Ports	1	1
6	Unconstrained Output Port Paths	1	1