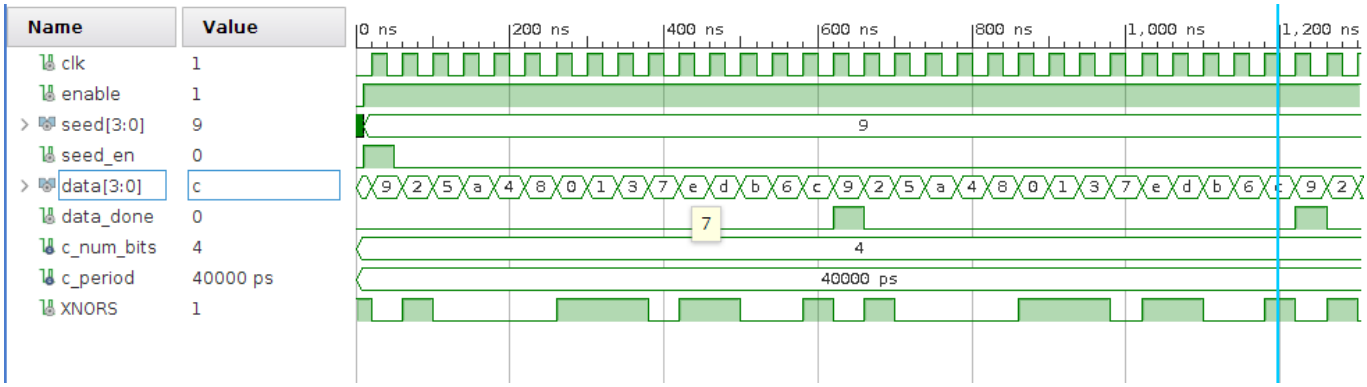
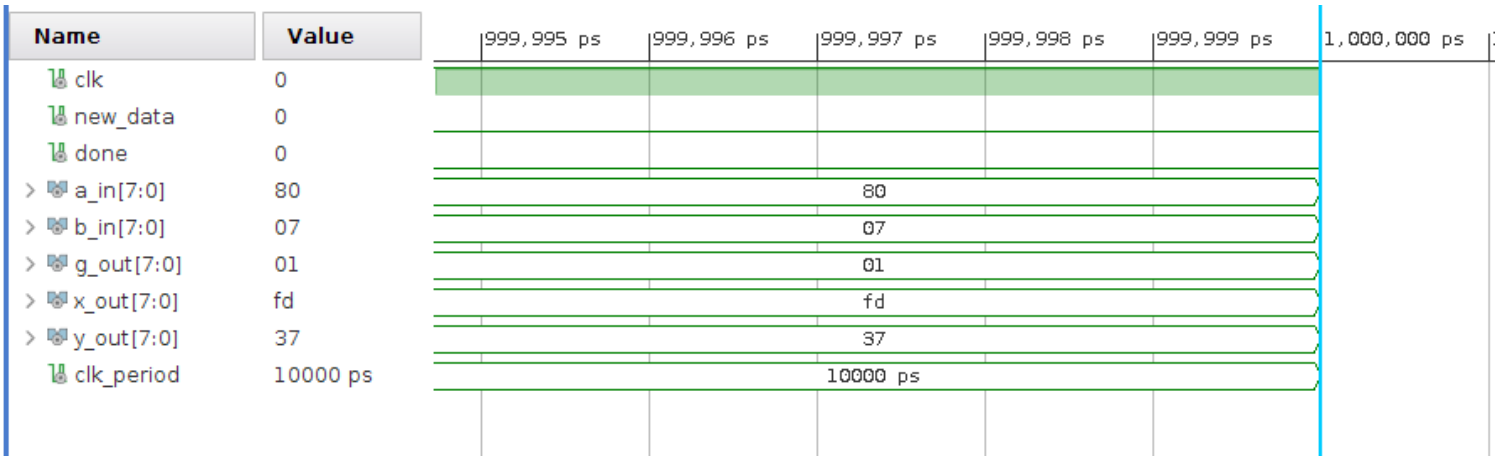
Part 1 : Waveforms

Appendix A



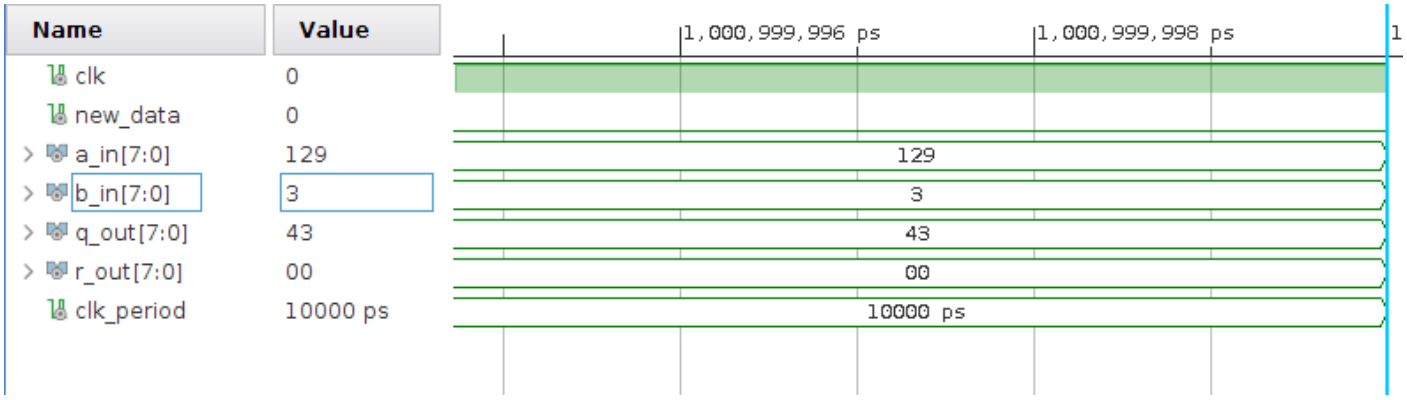
LFSR Waveform: note the seed_en tick, the data_done tick, and data, the stream of random values

Appendix B



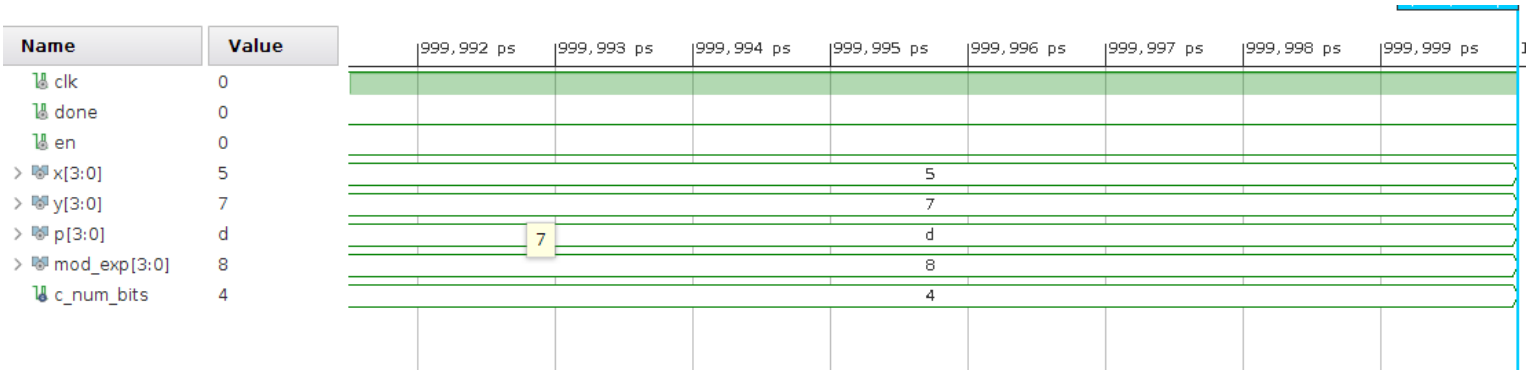
Extended GCD waveform: note a and b are coprime (g_out = 1)

Appendix C



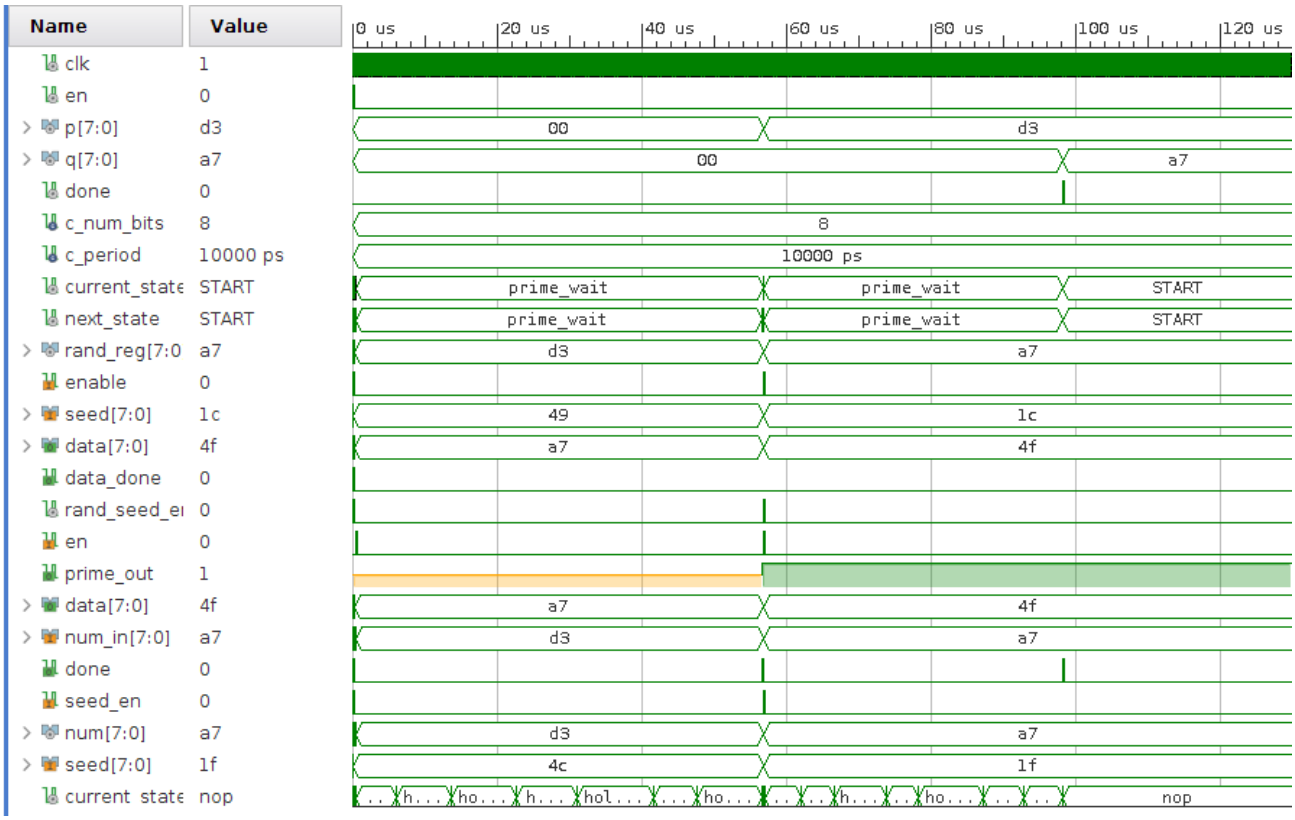
Modulus Waveform: note that 129/3 = 43 and
129 % 3 = 0

Appendix D



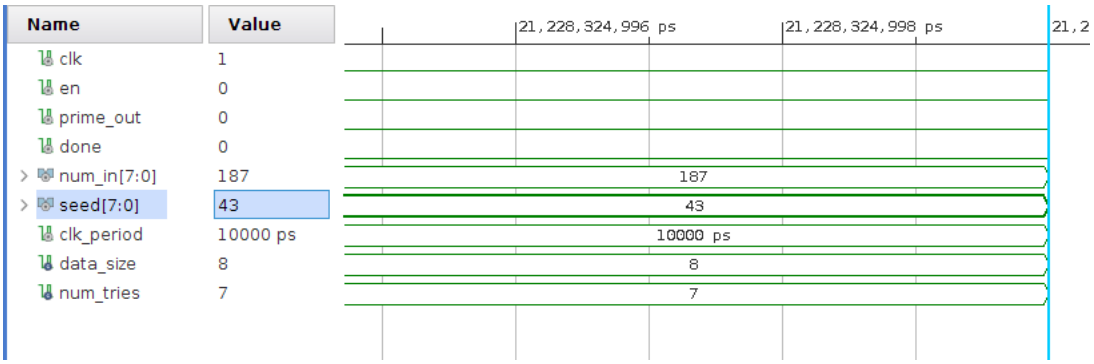
Modular Exponentiation Waveform: note that
x^y % p = mod_exp

Appendix E



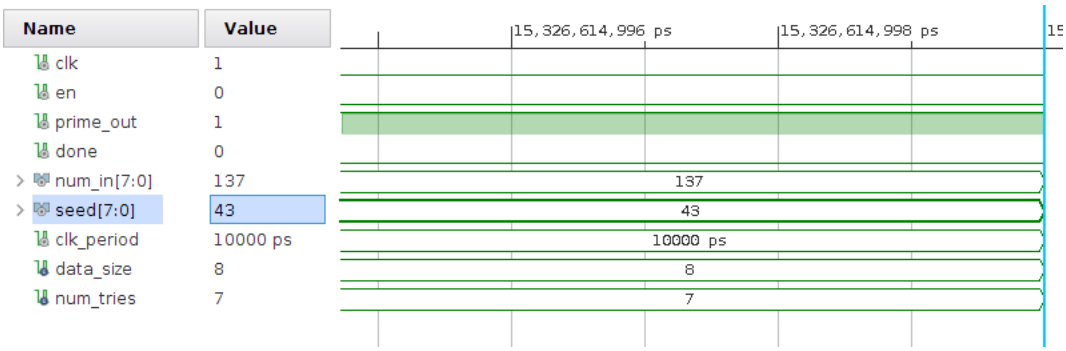
PQ Generation Waveform: note that p and q both get prime values

Appendix F



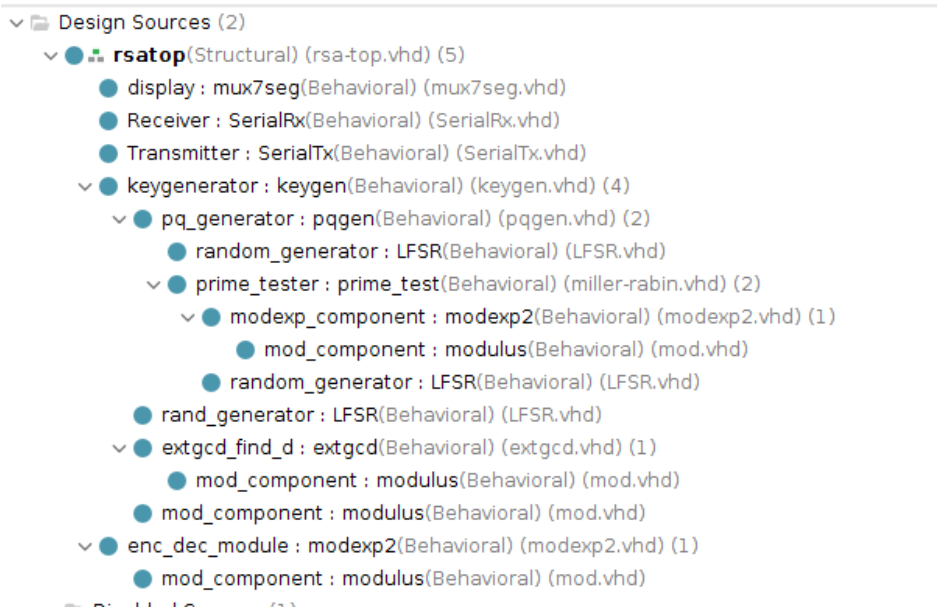
Rabin-Miller Primality Waveform 187 is not prime -> prime_out = 0

Appendix G



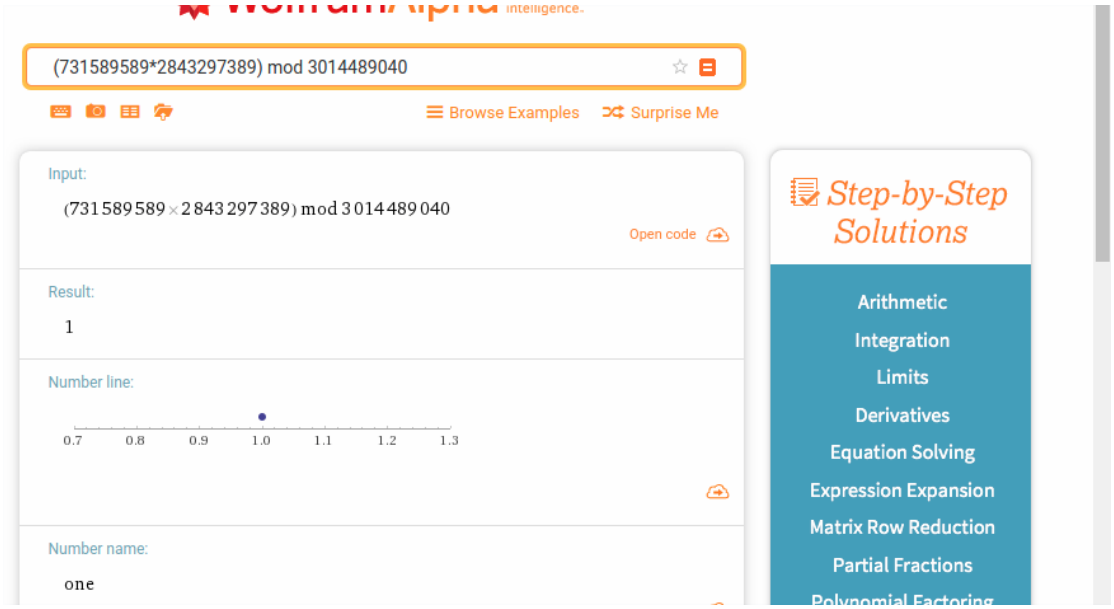
Miller-Rabin Primality Waveform: 137 is prime
-> prime_out = 1

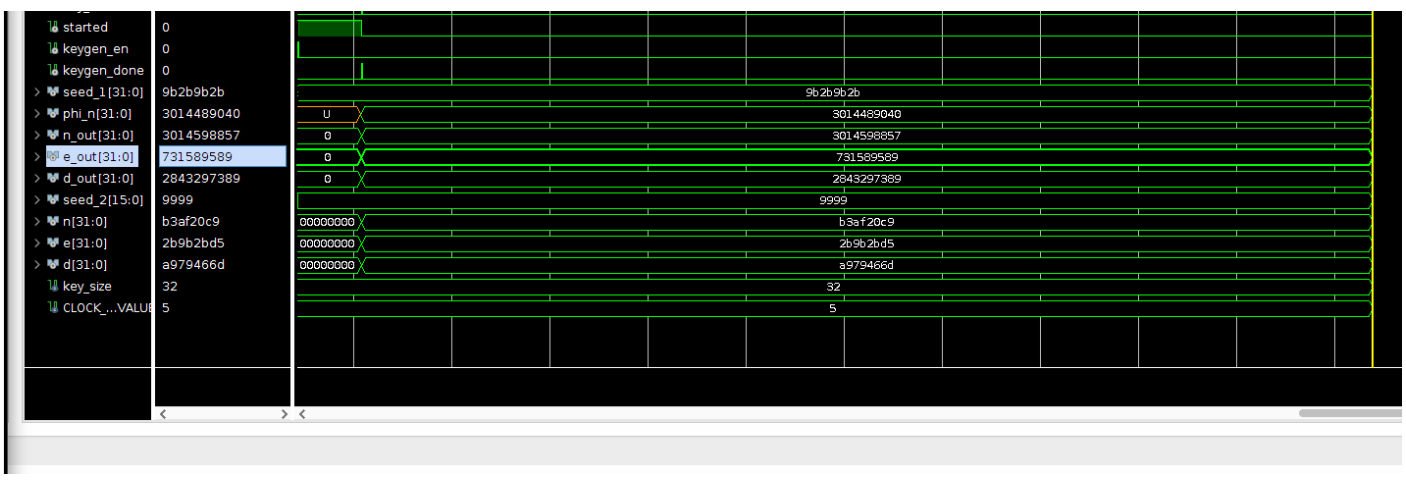
Appendix H



rsatop (entire project) hierarchy: Look at the modularization of components

Appendix I





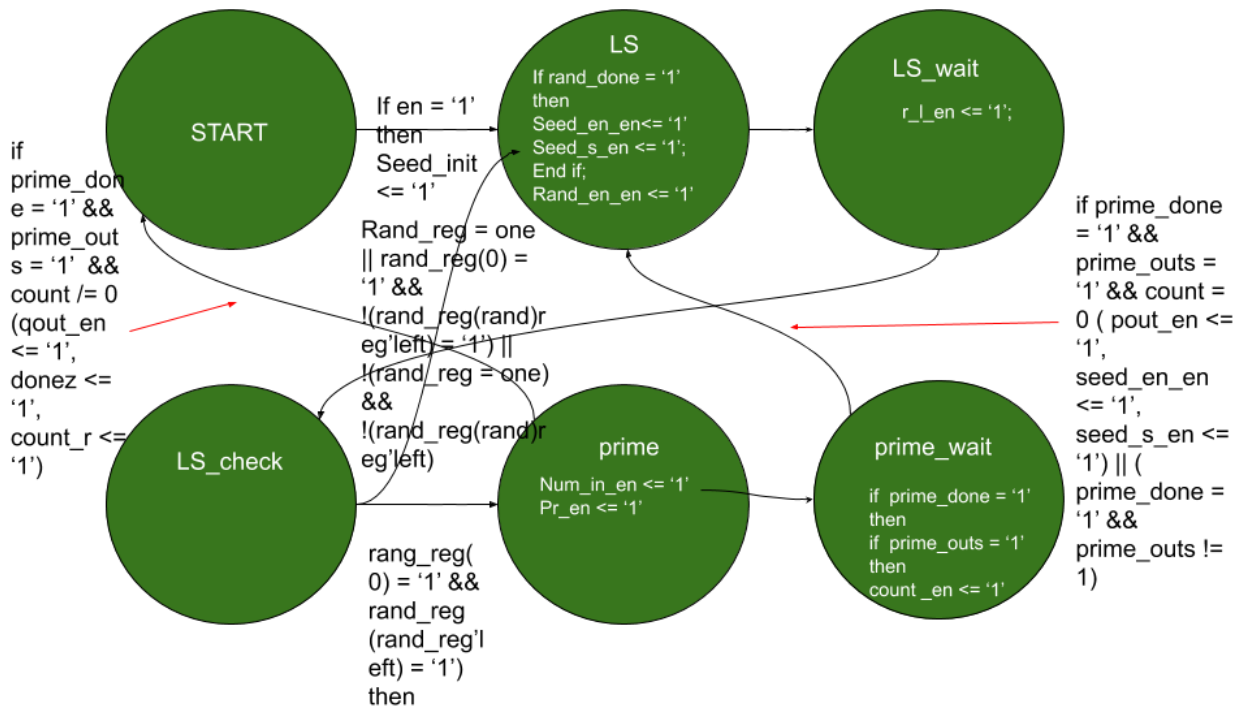
Generate key: Proof that our keys are correct. (e*d)modn = 1, as a property of RSA. Wolfram Alpha affirms this is the case

Appendix J

SerialRx Waveform: Look at rx_data, that's the finial value after the second RsRx packet

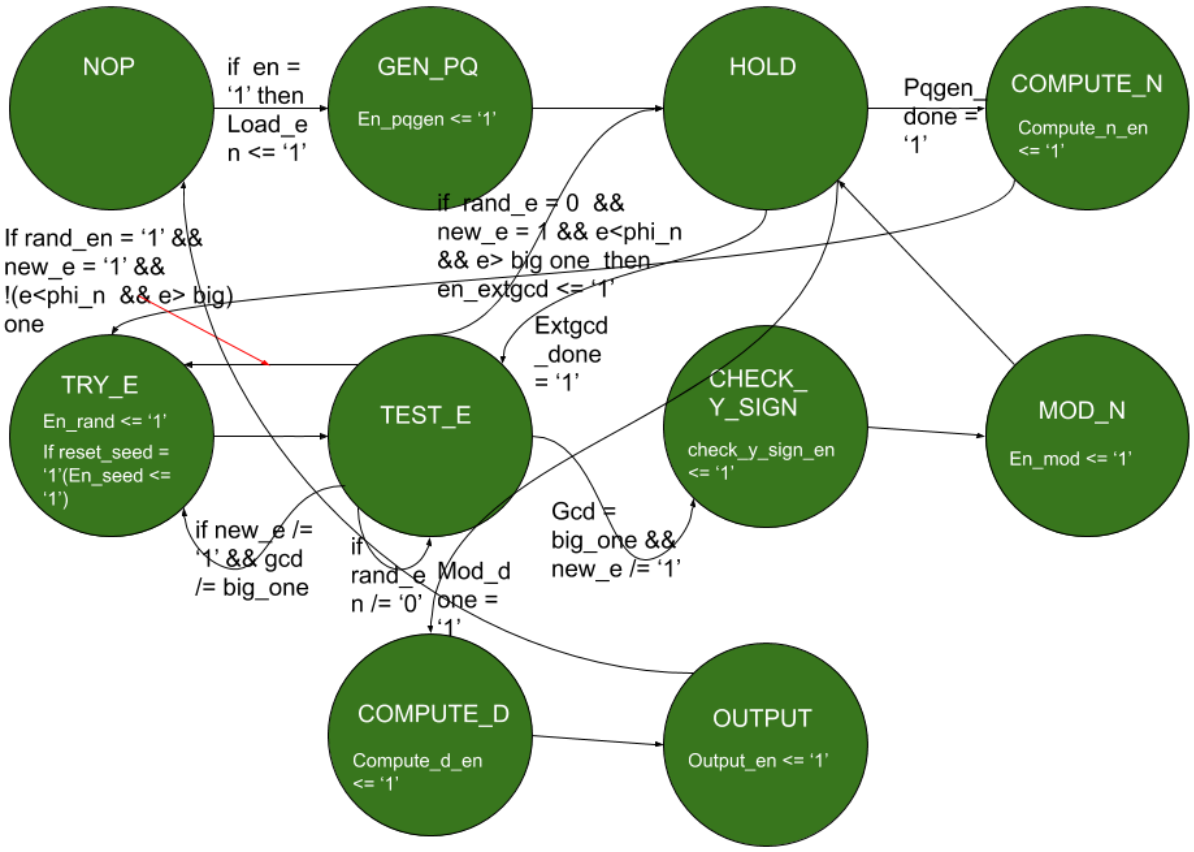
Part 2: State Machines

Appendix K



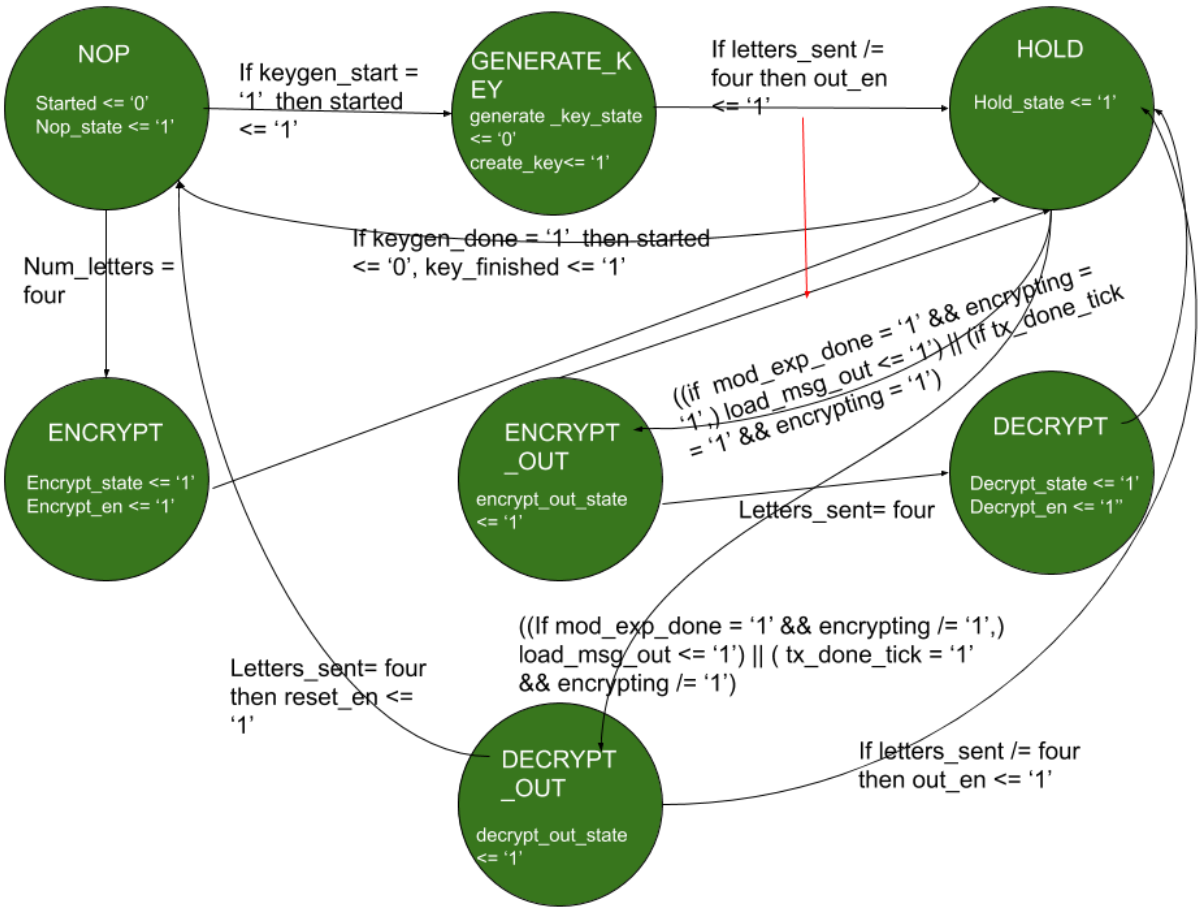
PQ Generation State Machine

Appendix L



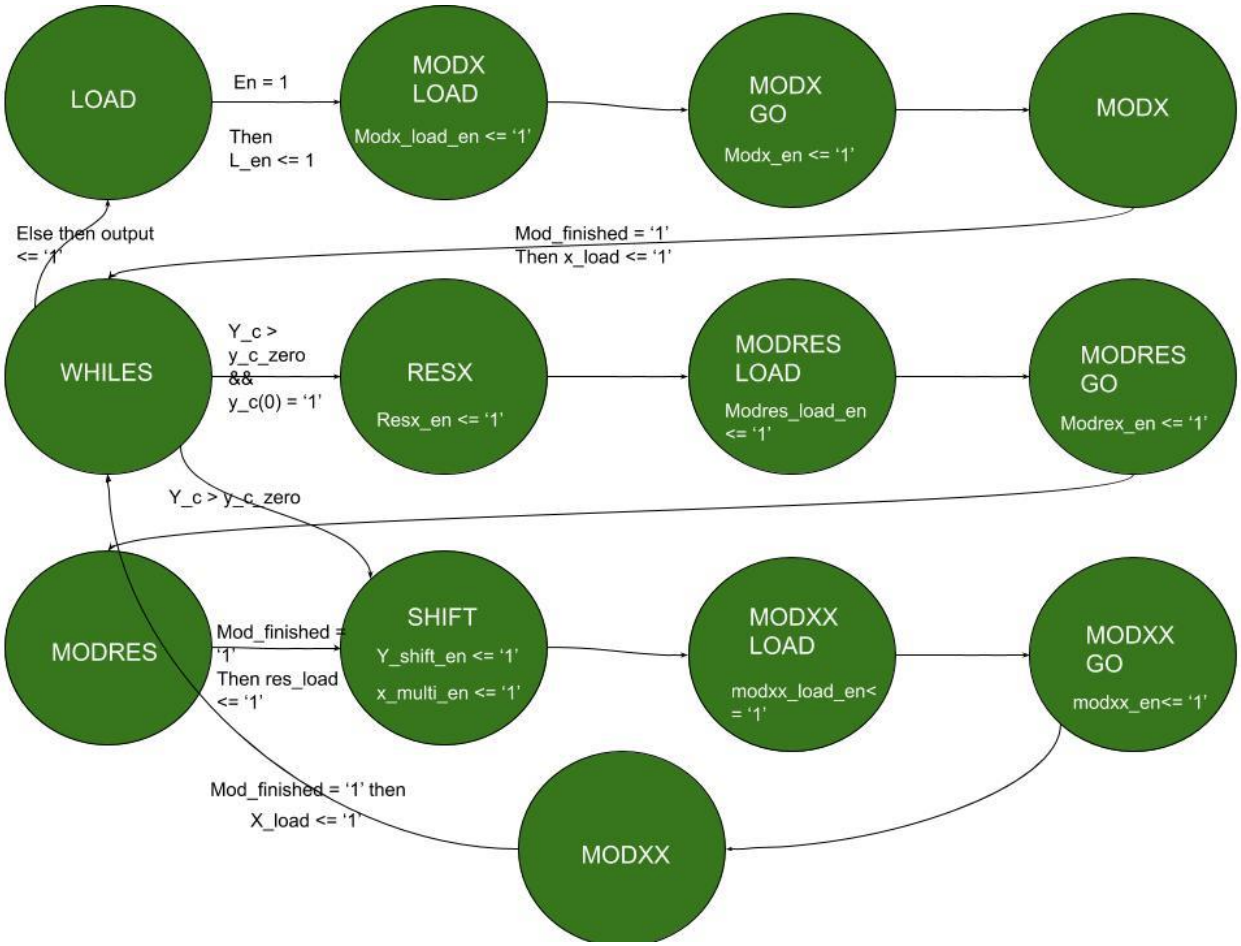
Key Generation State Machine

Appendix M



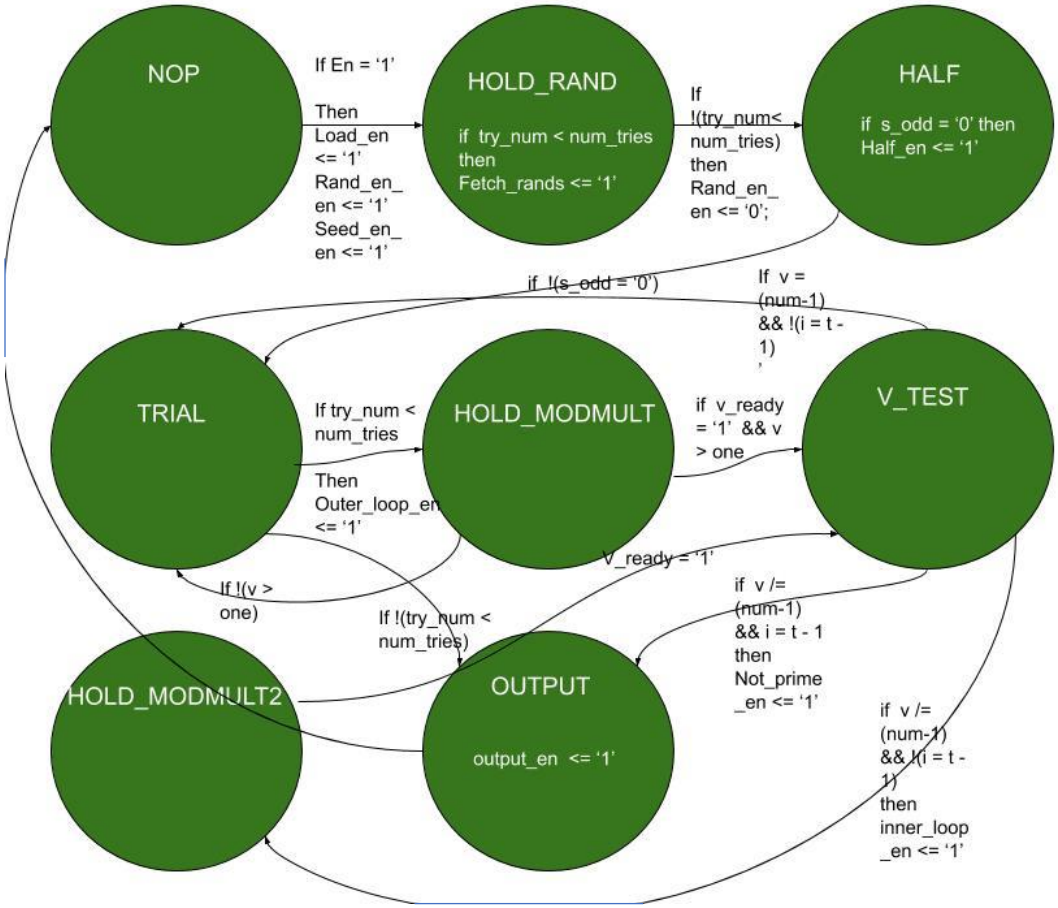
RSA Top State Machine

Appendix N



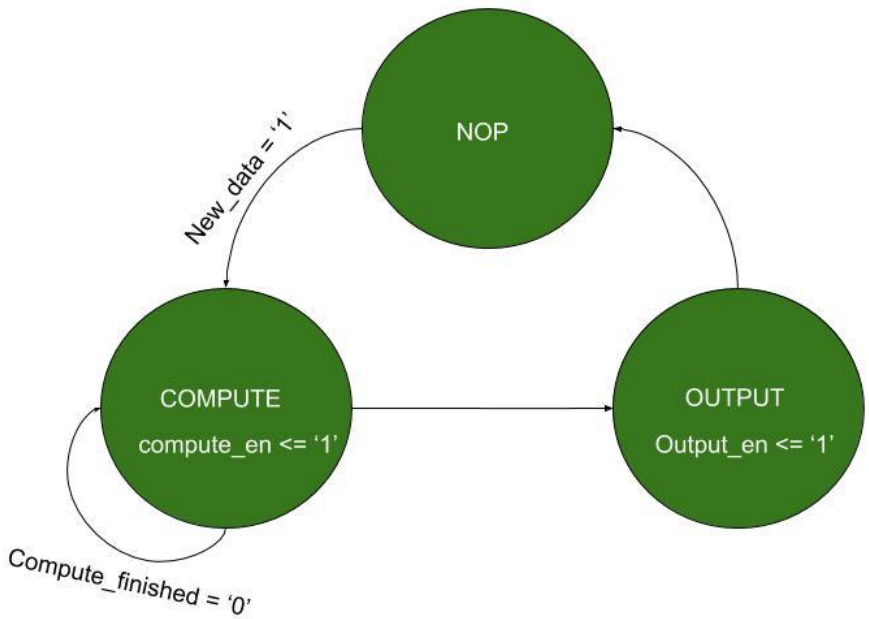
Modular
Exponentiation State

Appendix O



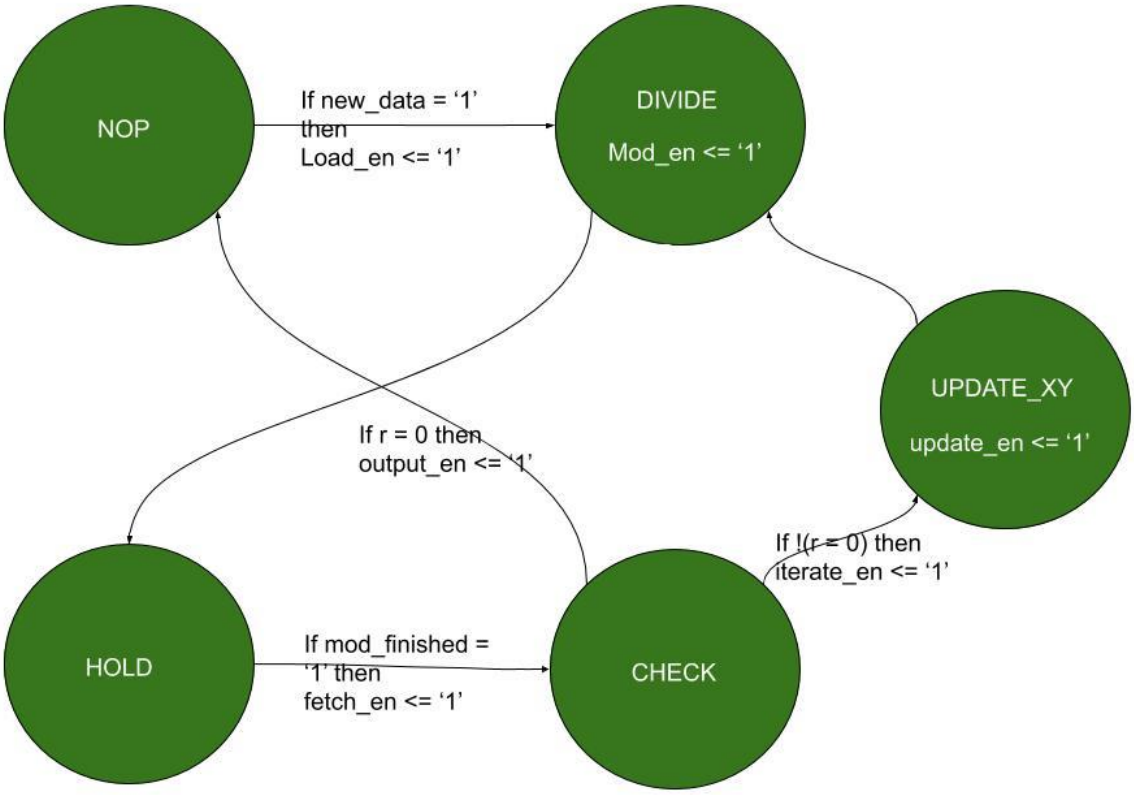
Rabin-Miller State Machine

Appendix P



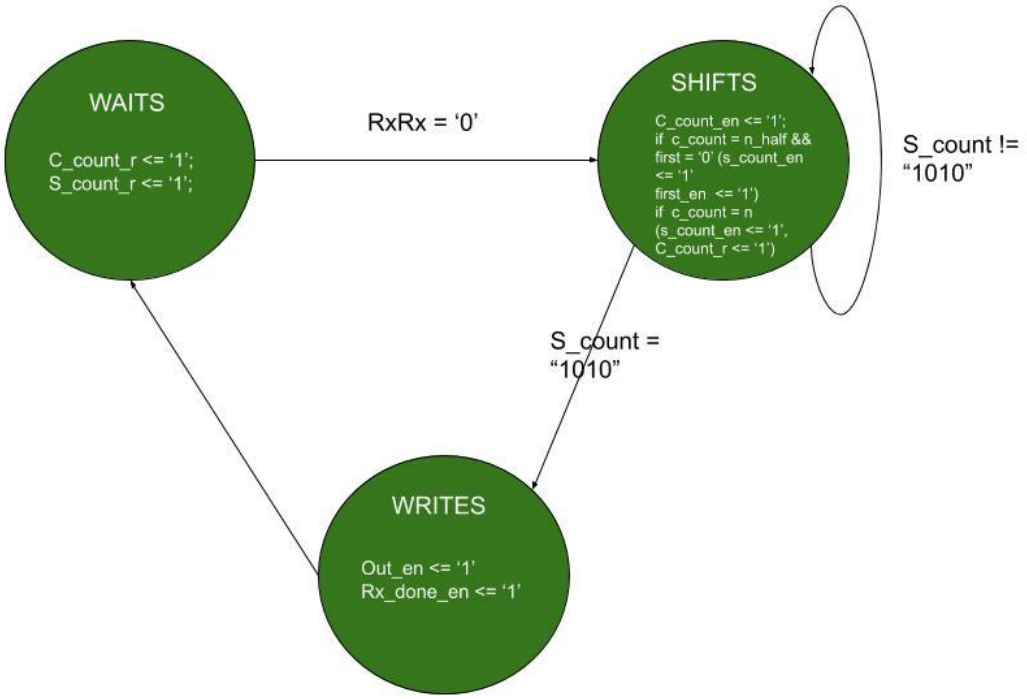
Modulus State Machine

Appendix Q



Extended GCD State Machine

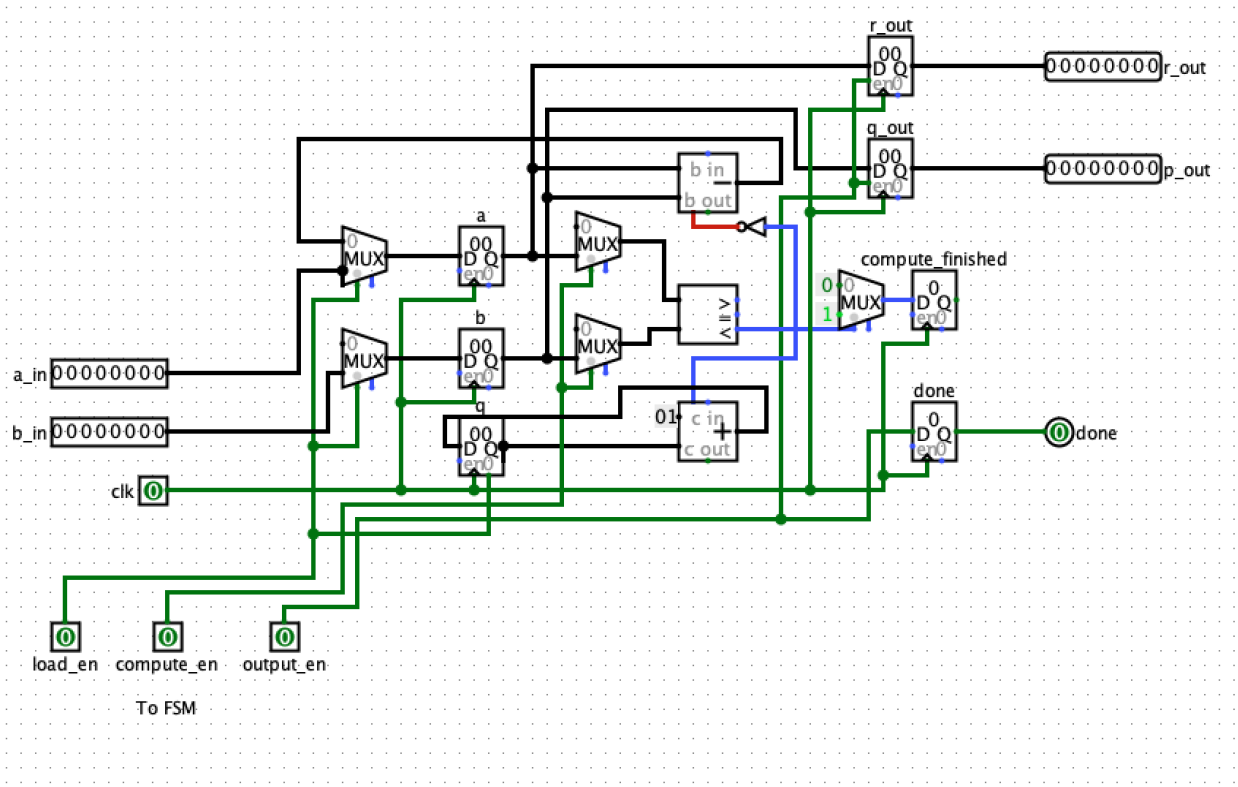
Appendix R



SerialRX State Machine

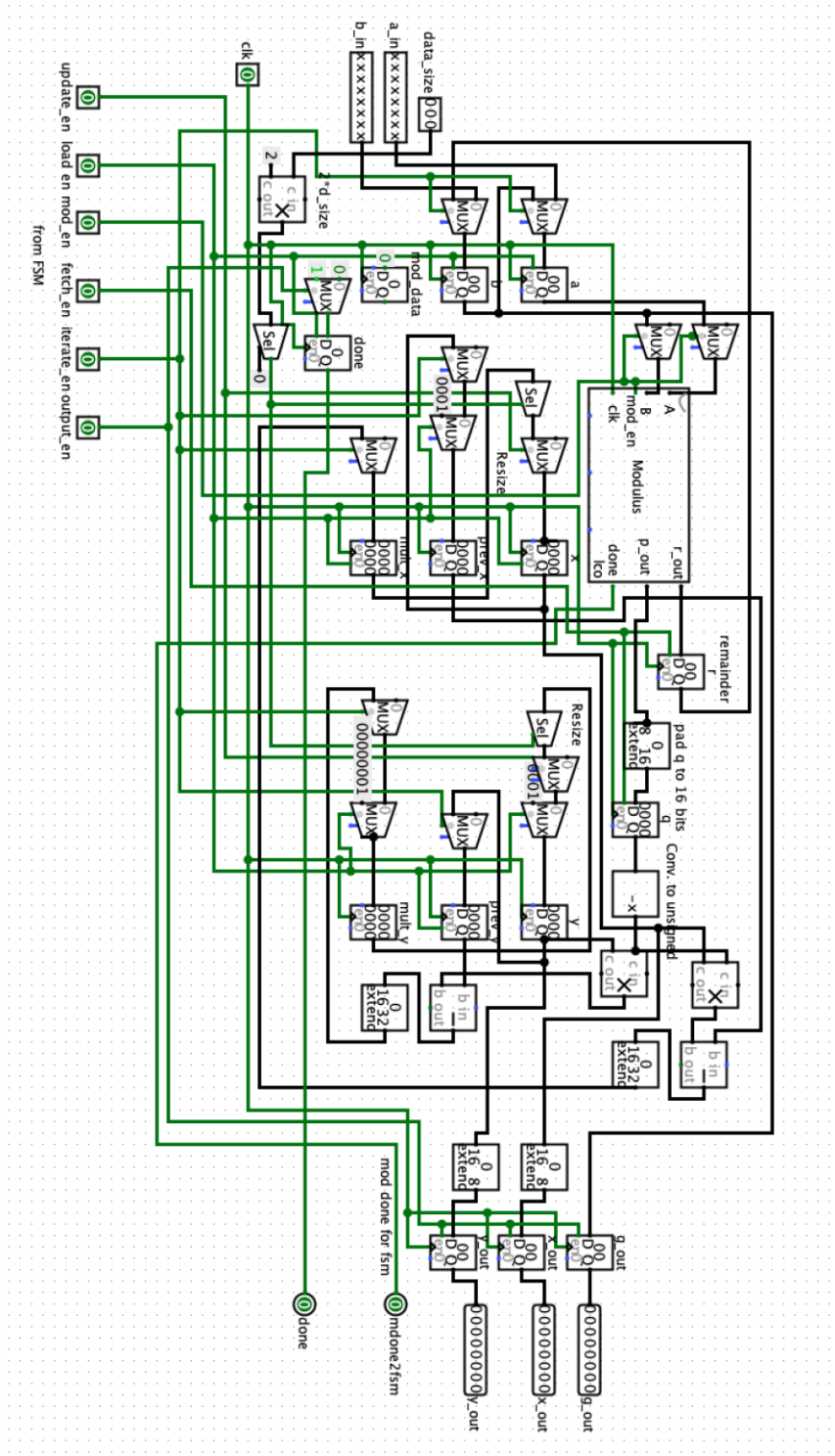
Part 3: Block Diagrams

Appendix S



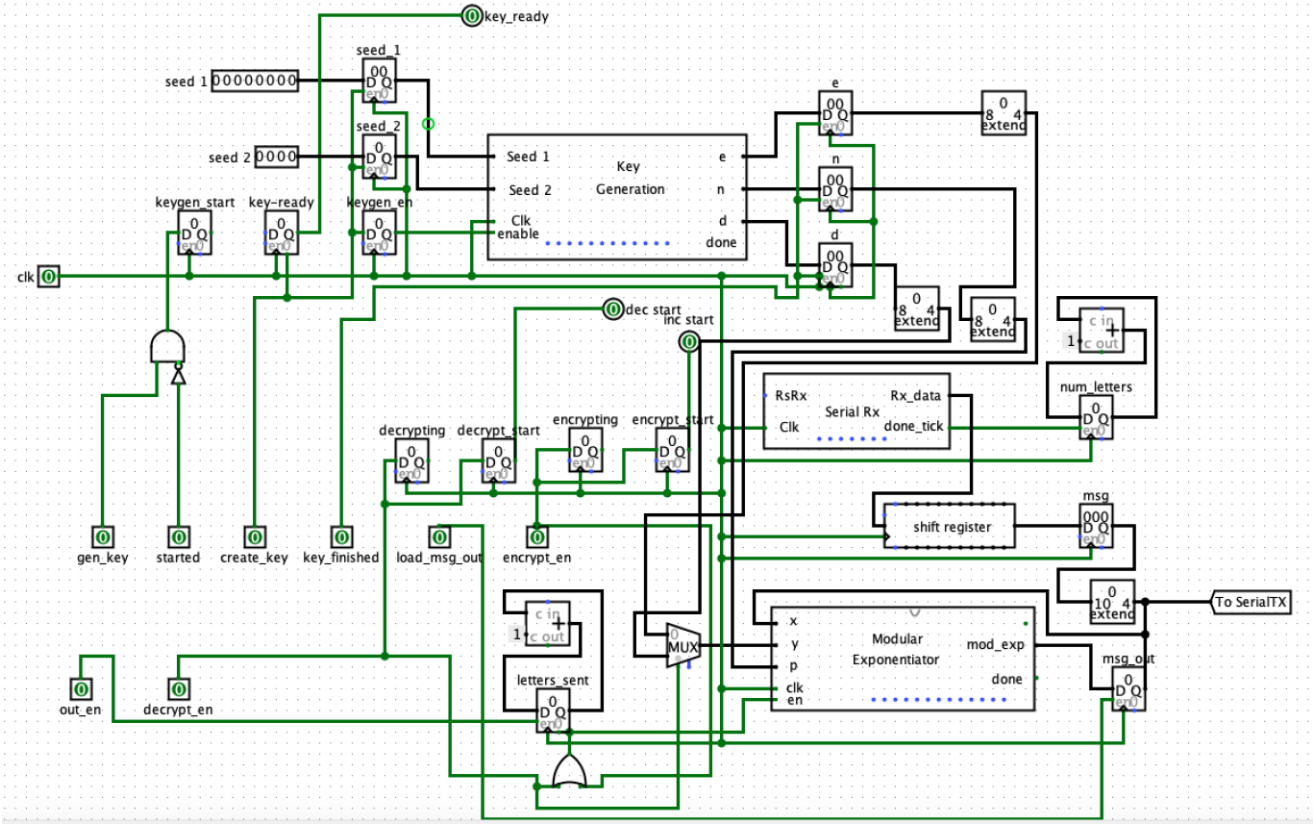
Modulus Block Diagram

Appendix T



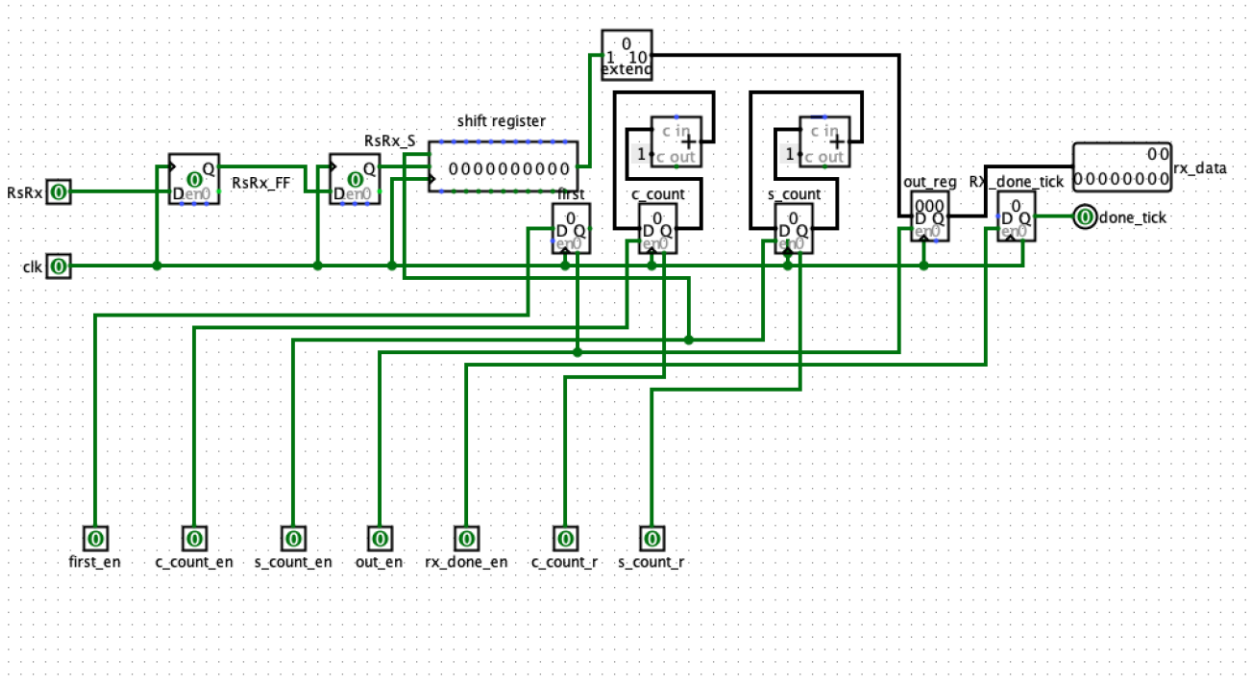
Block diagram of extended GCD

Appendix U



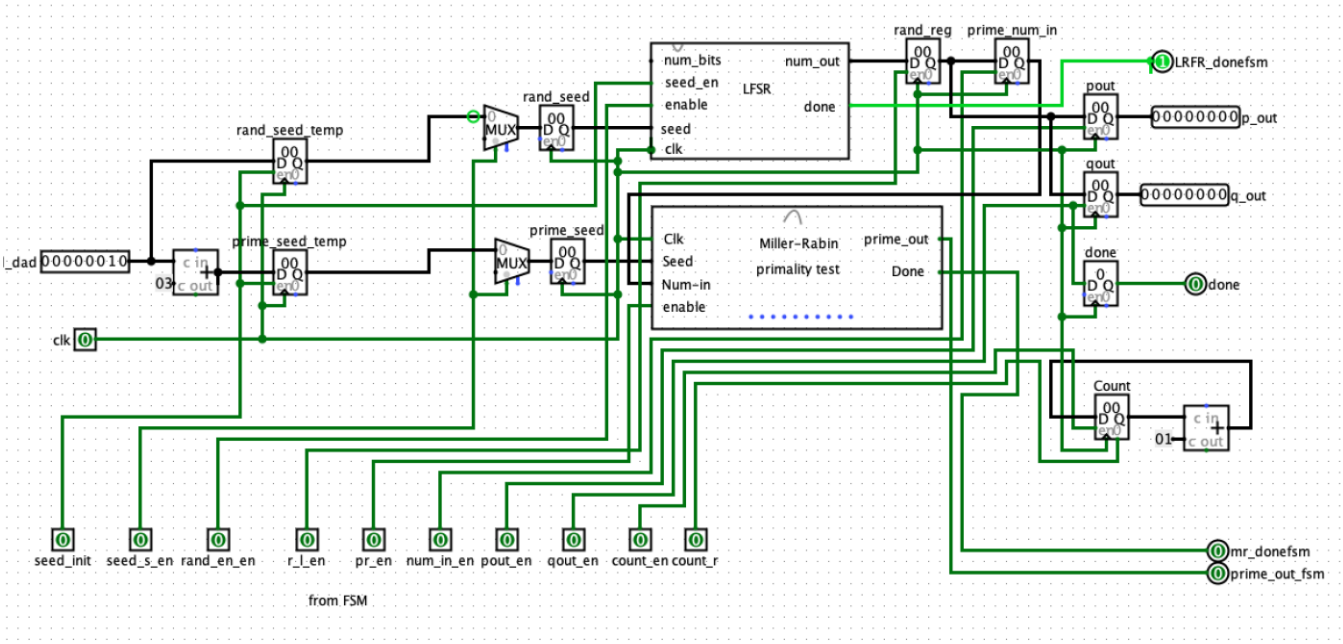
RSA top Block Diagram

Appendix V



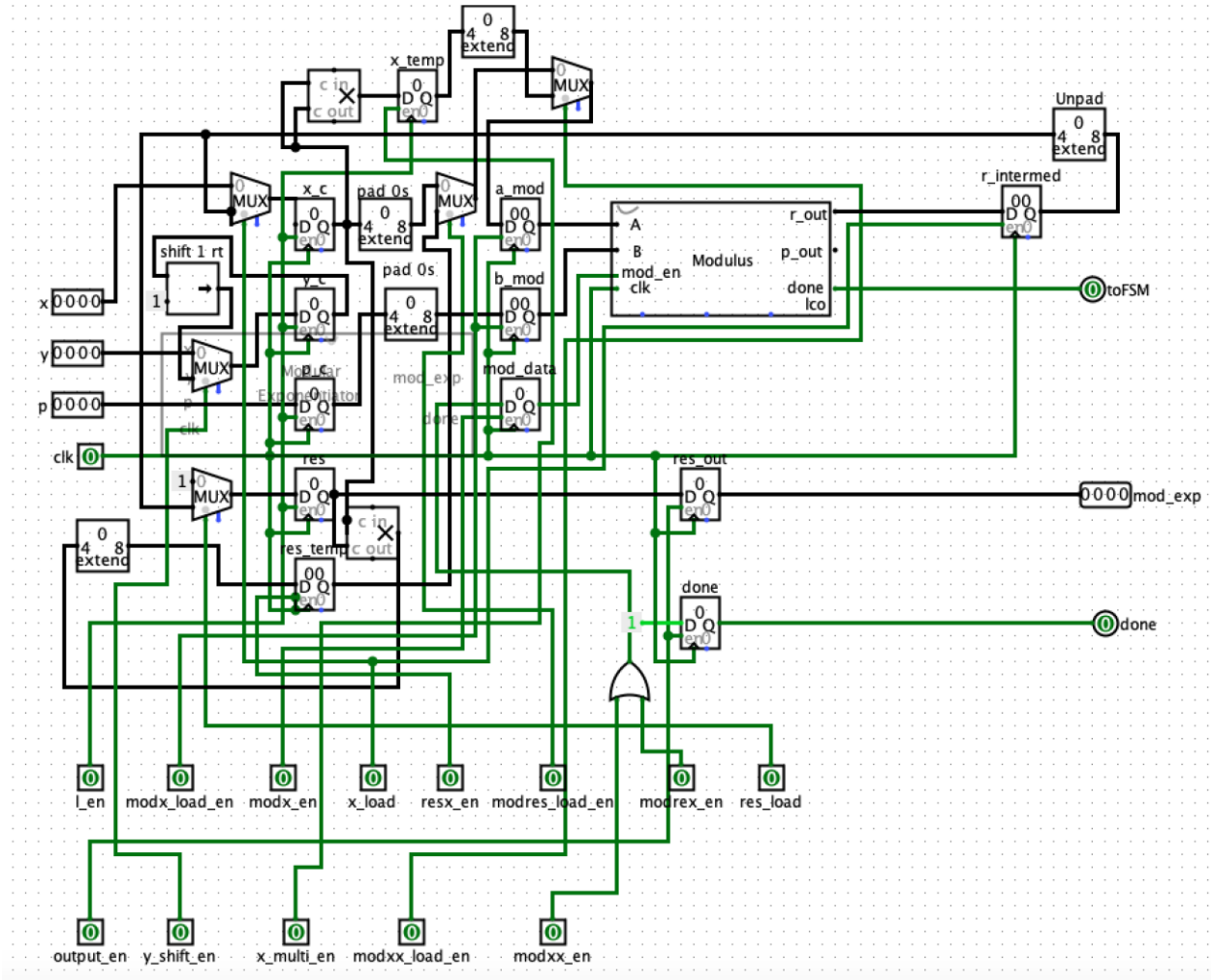
SerialRx Block Diagram

Appendix W



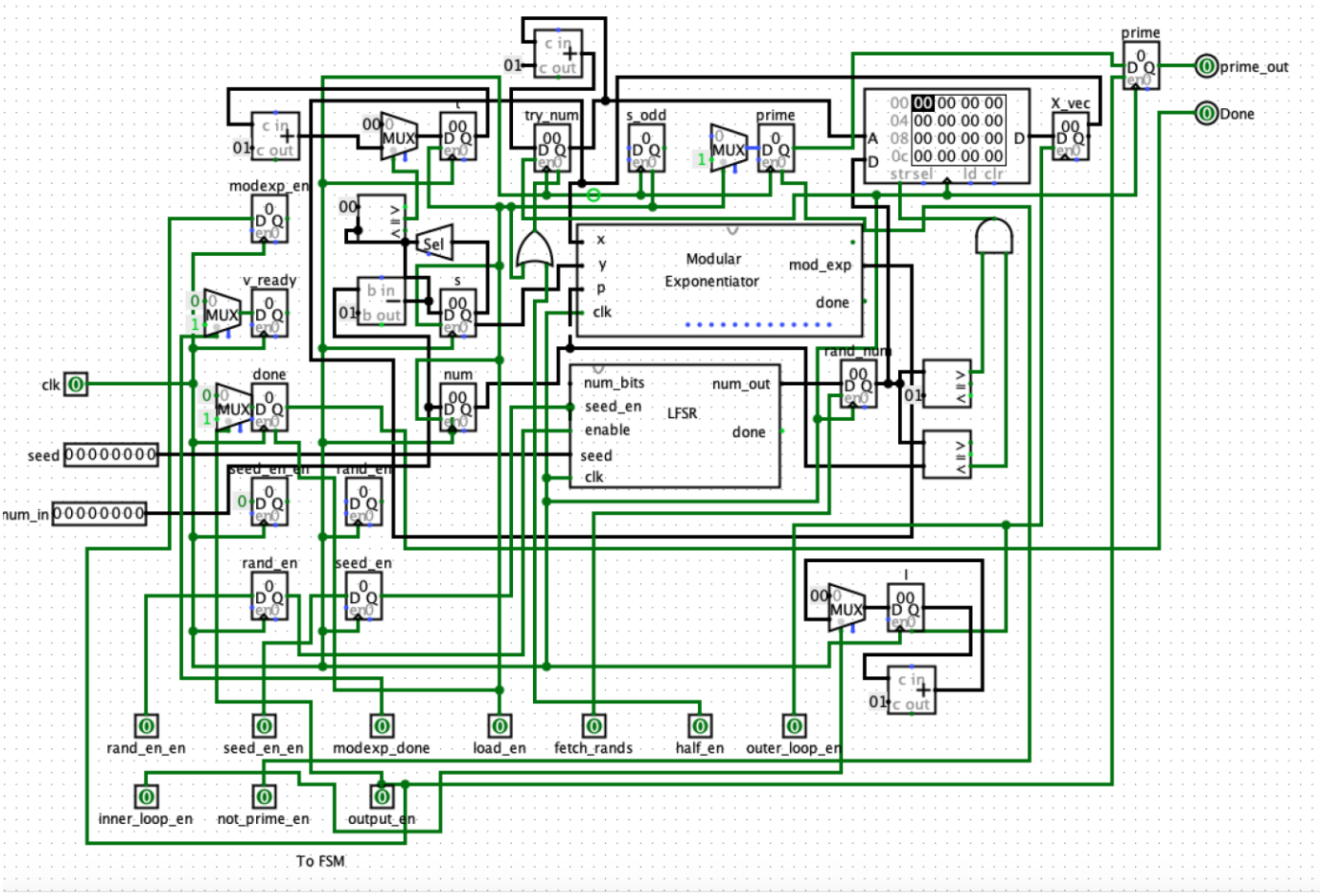
Pq Generation block diagram

Appendix X



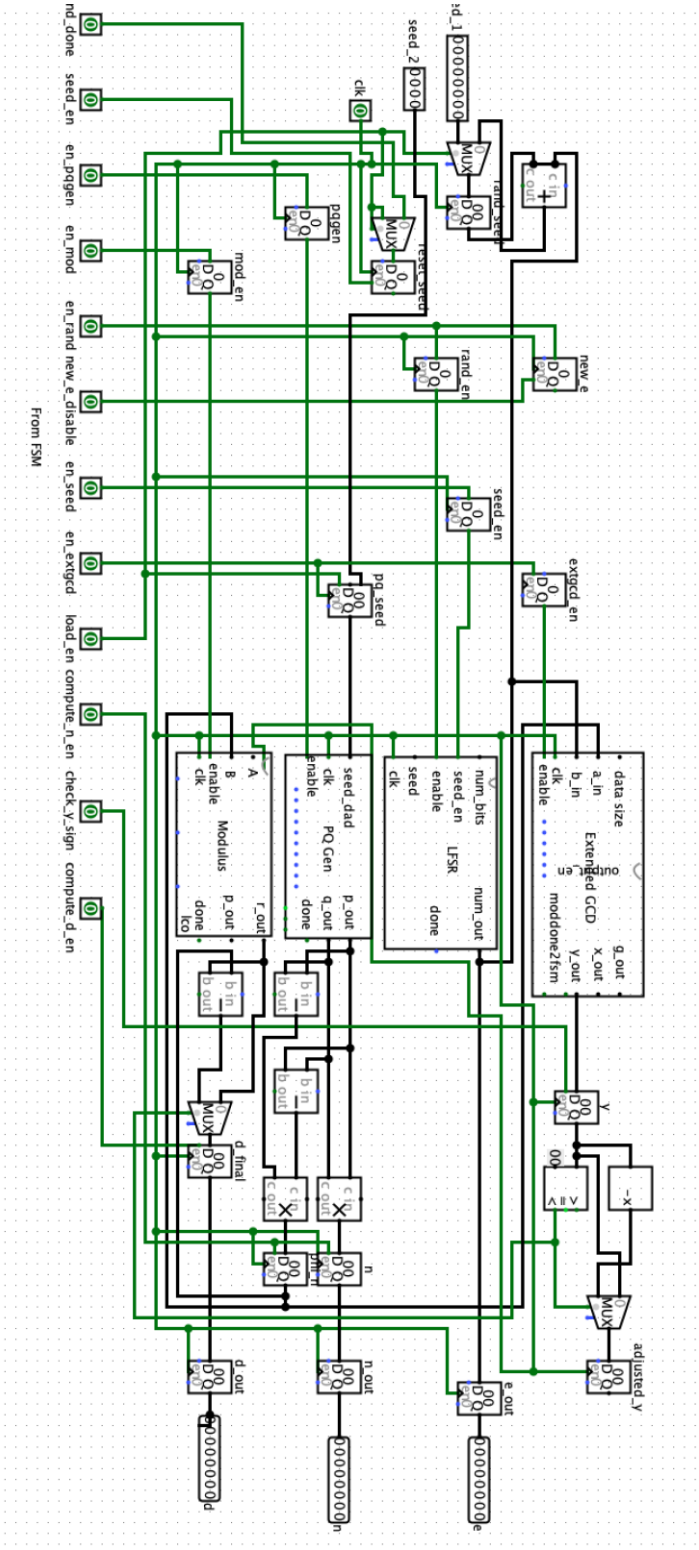
Modular Exponentiation Block Diagram

Appendix Y



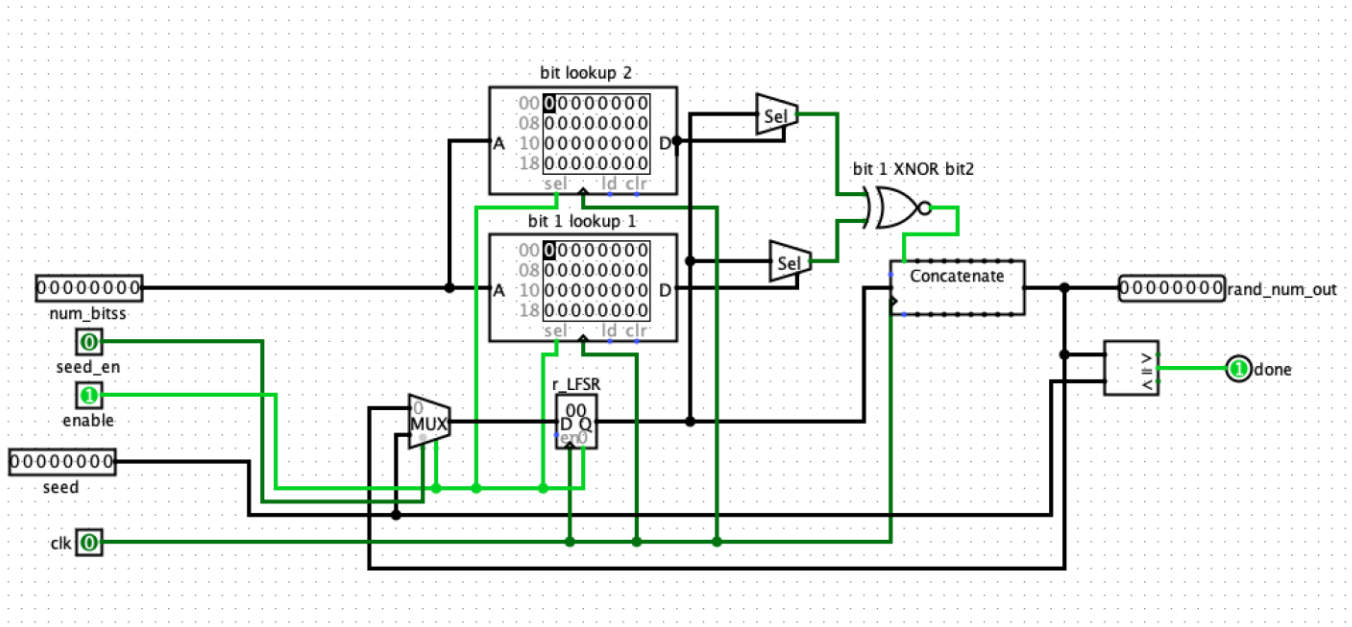
Rabin- Miller Block Diagram

Appendix Z



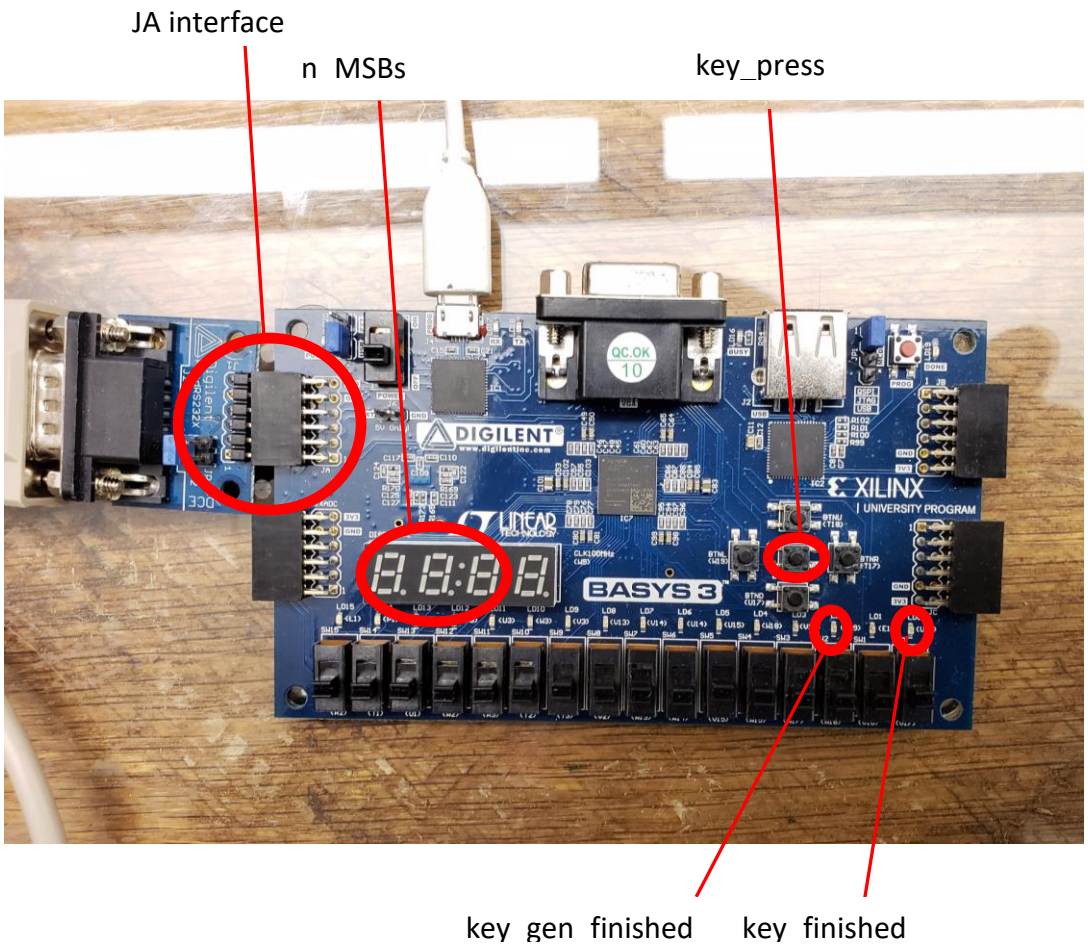
Key Generation Block Diagram

Appendix AA



LFSR Block Diagram

Appendix AB


JA interface
n MSBs
key_press
key gen finished
key finished
DIGILENT
XILINX
UNIVERSITY PROGRAM
BASYS 3

Appendix AC

Resource Utilization

| Tool Version : Vivado v.2018.3 (lin64) Build 2405991 Thu Dec 6 23:36:41 MST 2018
| Date : Tue Jun 4 13:39:19 2019
| Host : mkarch running 64-bit Antergos Linux
| Command : report_utilization -file rsatop_utilization_synth.rpt -pb rsatop_utilization_synth.pb
| Design : rsatop
| Device : 7a35tcpg236-2
| Design State : Synthesized

Utilization Design Information

Table of Contents
---
1. Slice Logic
1.1 Summary of Registers by Type
2. Memory
3. DSP
4. IO and GT Specific
5. Clocking
6. Specific Feature
7. Primitives
8. Black Boxes
9. Instantiated Netlists

1. Slice Logic

Site Type	Used	Fixed	Available	Util%
Slice LUTs*	1729	0	20800	8.31
LUT as Logic	1713	0	20800	8.24
LUT as Memory	16	0	9600	0.17
LUT as Distributed RAM	16	0		
LUT as Shift Register	0	0		
Slice Registers	2137	0	41600	5.14
Register as Flip Flop	2135	0	41600	5.13
Register as Latch	2	0	41600	<0.01
F7 Muxes	0	0	16300	0.00

```
| F8 Muxes                    |    0 |     0 |      8150 |  0.00 |
+-----------------------------+------+-------+-----------+-------+
```

* Warning! The Final LUT count, after physical optimizations and full implementation, is typically lower. Run opt_design after synthesis, if not already completed, for a more realistic count.

1.1 Summary of Registers by Type

```
+-------+--------------+-------------+--------------+
| Total | Clock Enable | Synchronous | Asynchronous |
+-------+--------------+-------------+--------------+
| 0     |            _ |           - |            - |
| 0     |            _ |           - |          Set |
| 0     |            _ |           - |        Reset |
| 0     |            _ |         Set |            - |
| 0     |            _ |       Reset |            - |
| 0     |          Yes |           - |            - |
| 0     |          Yes |           - |          Set |
| 2     |          Yes |           - |        Reset |
| 6     |          Yes |         Set |            - |
| 2129  |          Yes |       Reset |            - |
+-------+--------------+-------------+--------------+
```

2. Memory

```
+----------------+------+-------+-----------+-------+
|    Site Type   | Used | Fixed | Available | Util% |
+----------------+------+-------+-----------+-------+
| Block RAM Tile |    0 |     0 |        50 |  0.00 |
|   RAMB36/FIFO* |    0 |     0 |        50 |  0.00 |
|   RAMB18       |    0 |     0 |       100 |  0.00 |
+----------------+------+-------+-----------+-------+
```

* Note: Each Block RAM Tile only has one FIFO logic available and therefore can accommodate only one FIFO36E1 or one FIFO18E1. However, if a FIFO18E1 occupies a Block RAM Tile, that tile can still accommodate a RAMB18E1

3. DSP

```
+----------------+------+-------+-----------+-------+
|    Site Type   | Used | Fixed | Available | Util% |
```

DSPs	29	0	90	32.22
DSP48E1 only	29			

4. IO and GT Specific

Site Type	Used	Fixed	Available	Util%
Bonded IOB	26	0	106	24.53
Bonded IPADs	0	0	10	0.00
Bonded OPADs	0	0	4	0.00
PHY_CONTROL	0	0	5	0.00
PHASER_REF	0	0	5	0.00
OUT_FIFO	0	0	20	0.00
IN_FIFO	0	0	20	0.00
IDELAYCTRL	0	0	5	0.00
IBUFDS	0	0	104	0.00
GTPE2_CHANNEL	0	0	2	0.00
PHASER_OUT/PHASER_OUT_PHY	0	0	20	0.00
PHASER_IN/PHASER_IN_PHY	0	0	20	0.00
IDELAYE2/IDELAYE2_FINEDELAY	0	0	250	0.00
IBUFDS_GTE2	0	0	2	0.00
ILOGIC	0	0	106	0.00
OLOGIC	0	0	106	0.00

5. Clocking

Site Type	Used	Fixed	Available	Util%
BUFGCTRL	3	0	32	9.38
BUFIO	0	0	20	0.00
MMCME2_ADV	0	0	5	0.00
PLLE2_ADV	0	0	5	0.00
BUFMRCE	0	0	10	0.00
BUFHCE	0	0	72	0.00
BUFR	0	0	20	0.00

6. Specific Feature

Site Type	Used	Fixed	Available	Util%
BSCANE2	0	0	4	0.00
CAPTUREE2	0	0	1	0.00
DNA_PORT	0	0	1	0.00
EFUSE_USR	0	0	1	0.00
FRAME_ECCE2	0	0	1	0.00
ICAPE2	0	0	2	0.00
PCIE_2_1	0	0	1	0.00
STARTUPE2	0	0	1	0.00
XADC	0	0	1	0.00

7. Primitives

Ref Name	Used	Functional Category
FDRE	2129	Flop & Latch
LUT2	470	LUT
LUT3	439	LUT
LUT4	428	LUT
LUT5	291	LUT
CARRY4	255	CarryLogic
LUT6	248	LUT
LUT1	163	LUT
DSP48E1	29	Block Arithmetic
OBUF	23	IO
RAMS32	16	Distributed Memory
FDSE	6	Flop & Latch
IBUF	3	IO
BUFG	3	Clock
LDCE	2	Flop & Latch

8. Black Boxes

```
+----------+------+
| Ref Name | Used |
+----------+------+
```

9. Instantiated Netlists

```
+----------+------+
| Ref Name | Used |
+----------+------+
```

Appendix AD
Explanation of remaining top level synthesis errors

Synthesis (120 warnings)
- [Synth 8-327] inferring latch for variable 'rand_en_en_reg' [miller-rabin.vhd:146] (1 more like this)
- [Synth 8-6014] Unused sequential element was removed. [extgcd.vhd:192] (11 more like this)
- [Synth 8-3936] Found unconnected internal register 'prime_tester/modexp_component/mod_component/r_out_reg' and it is trimmed from '32' to '16' bits. [mod.vhd:120] (1 more like this)
- [Synth 8-3917] design rsatop has port generate_key_state driven by constant 0 (2 more like this)
- [Synth 8-3332] Sequential element (i_2) is unused and will be removed from module keygen. (99 more like this)
- [Constraints 18-5210] No constraints selected for write.
  Resolution: This message can indicate that there are no constraints for the design, or it can indicate that the used_in flags are set such that the constraints are ignored. This later case is used when running synth_design to not write synthesis co
  resulting checkpoint. Instead, project constraints are read when the synthesized design is opened.

Synth 8-327: Rand_en_en is intended to be a latch for an enable bit that must change between states, irrelevant of clock
Synth 8-6014: Sequential element because extgcd is instantiated with signals off generic types.
Synth 8-3936: Due to instantiation with generic types
Synth 8-3917: Constant 0 for a led light on the FPGA
Synth 8-3332: Keygen does not contain i_2. Confusing errors
Constraints: properly declared a constraint file