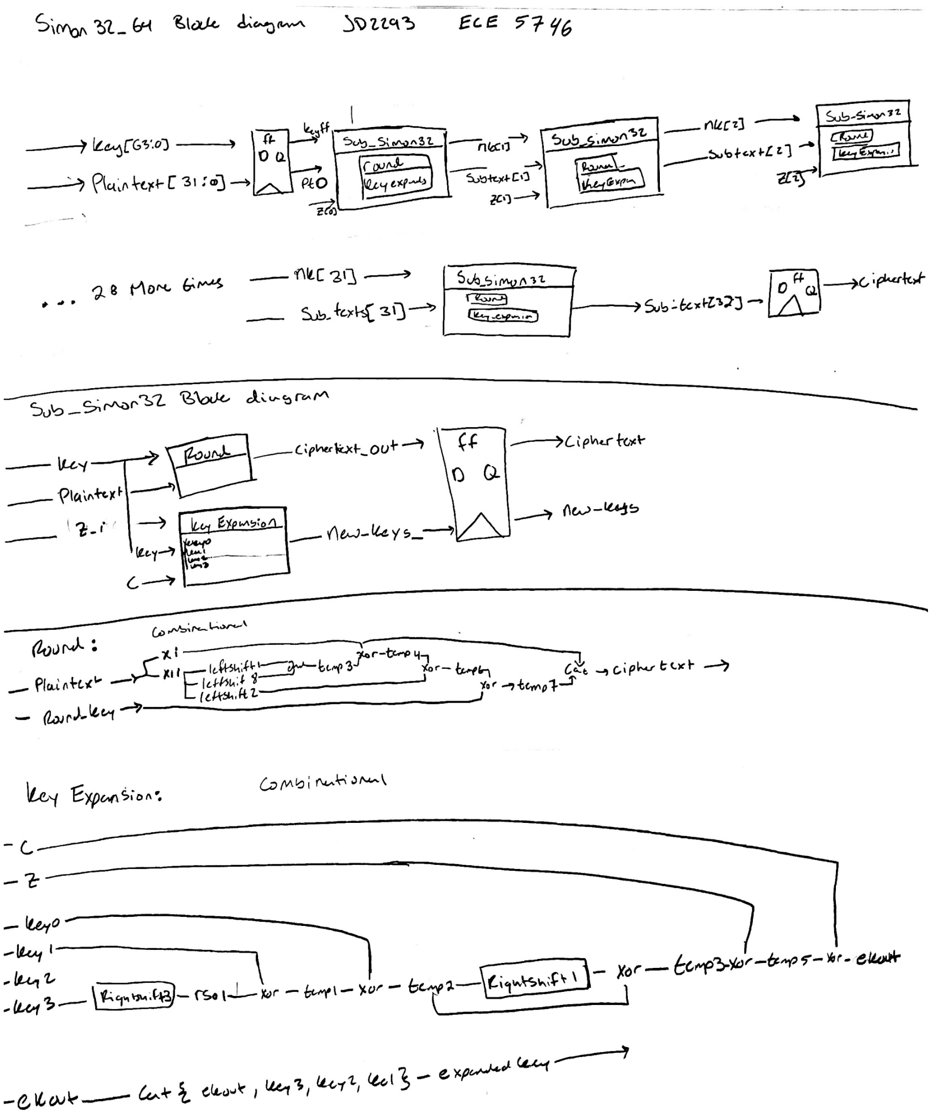
Block Diagram:



Design decision discussion:

The decisions for design of this chip tried to trade area for speed. It is clear from the Quality metric that more weight was put on the latency of the design. This led me to focus efforts on streamlining the original System Verilog that I had from milestone 1. In my milestone 1 SystemVerilog I had designed it without regard for timing, only function. This led to a slow design. During synthesis the clock period that was found was 240ps (I then used a period of for apr 288 which is 1.2 times 240). This design included 4 round modules at the start, which completed the first 4 rounds (each with a key of 16 bits), then went into a sub_simon32 module which computed the rounds and the key expansion in one. Each of these was wired together. This caused a slower clock period necessary however the final cipher key was ready at 28 cycles with 28 sub_simon32 modules.

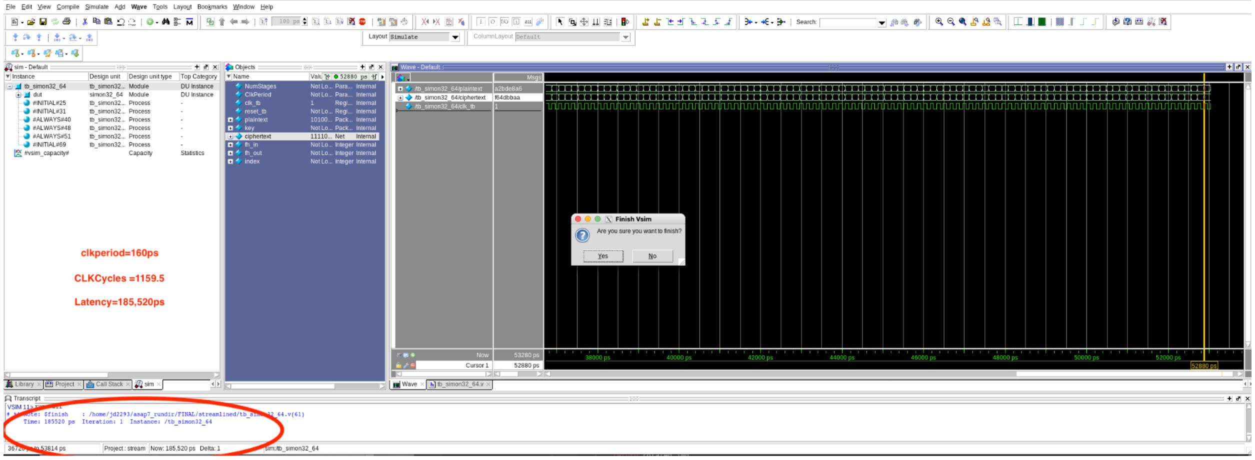
For the final milestone I went back and redesigned the SystemVerilog modules. After working with block diagram layouts I found that I could call the sub_simon32 module directly. I had to change how the round took keys, previously it took one 16 bit key at a time, now it takes a 64 bit key and works with only the first 16 bits. This allowed the sub_simon32 modules to be called directly after the first flip flop of input. I could then wire 32 sub_simon32 modules together. This allowed for immediate pipelining in the design. I have a flip flop at the output of sub_simon32 so that the subsequent rounds do not overlap. However the Round and Key_expansion within the sub_simon32 module can be computed concurrently, as I am relying on the key that was either given as input or computed previously by the previous sub_simon32 module.

I found that this design (while now needing 32 sub_simon modules and 32 cycles to complete) could run at a much faster clock period, for this submission I ran synthesis at 125ps and apr at 160ps. This was where I found most of my optimizations, by re-working the SystemVerilog.

The bottlenecks for this final design are definitely in power. I tried to push both the timing and area constraints. The quality metric for this design put more emphasis on the total latency, which is why my optimizations came from re-working system verilog. I do see how I could have pushed for a tighter area, since I see some space in the innovus layout. Also due to hiccups in the software we did not use the post layout Prime Time analysis tool. The main controls for which there was to optimize were: SystemVerilog code, Timing Constraint, Area constraints. From there I was able to solidify my design.

Label	**Value**	**Source**
Total Latency	0.00018552ms	Screenshot below
Clk period	160 ps	Params.vh
Clk cycles	1160	
Power	27.1 mW	power.rpt
Area (total area of core)	55.9066 mm^2	Summary.rpt
Innovus Density	.45	Summary (and screenshot below)
Number of Gates	[0] simon32_64 Gates=37268 Cells=8377 Area=26081.9 um^2	reportGateCount
Quality Metric	.000052145	

Jack Dempsey, JD2293, ECE 5746 Final Report



Layout Simulate

ColumnLayout Default

Instance	Design unit	Design unit type	Top Category
tb_simon32_64	tb_simon32...	Module	DU Instance
dut	simon32_64	Module	DU Instance
#INITIAL#25	tb_simon32...	Process	-
#INITIAL#31	tb_simon32...	Process	-
#ALWAYS#40	tb_simon32...	Process	-
#ALWAYS#48	tb_simon32...	Process	-
#ALWAYS#51	tb_simon32...	Process	-
#INITIAL#69	tb_simon32...	Process	-
#vsim_capacity#		Capacity	Statistics

Name	Valu 52880 ps		
NumStages	Not Lo...	Para...	Internal
ClkPeriod	Not Lo...	Para...	Internal
clk_tb	1	Regi...	Internal
reset_tb	Not Lo...	Regi...	Internal
plaintext	10100...	Pack...	Internal
key	Not Lo...	Pack...	Internal
ciphertext	11110...	Net	Internal
fh_in	Not Lo...	Integer	Internal
fh_out	Not Lo...	Integer	Internal
index	Not Lo...	Integer	Internal

	Msgs
/tb_simon32_64/plaintext	a2bde8a6
/tb_simon32_64/ciphertext	f64dbbaa
/tb_simon32_64/clk_tb	1
Now	53280 ps
Cursor 1	52880 ps

Finish Vsim

Are you sure you want to finish?

Yes No

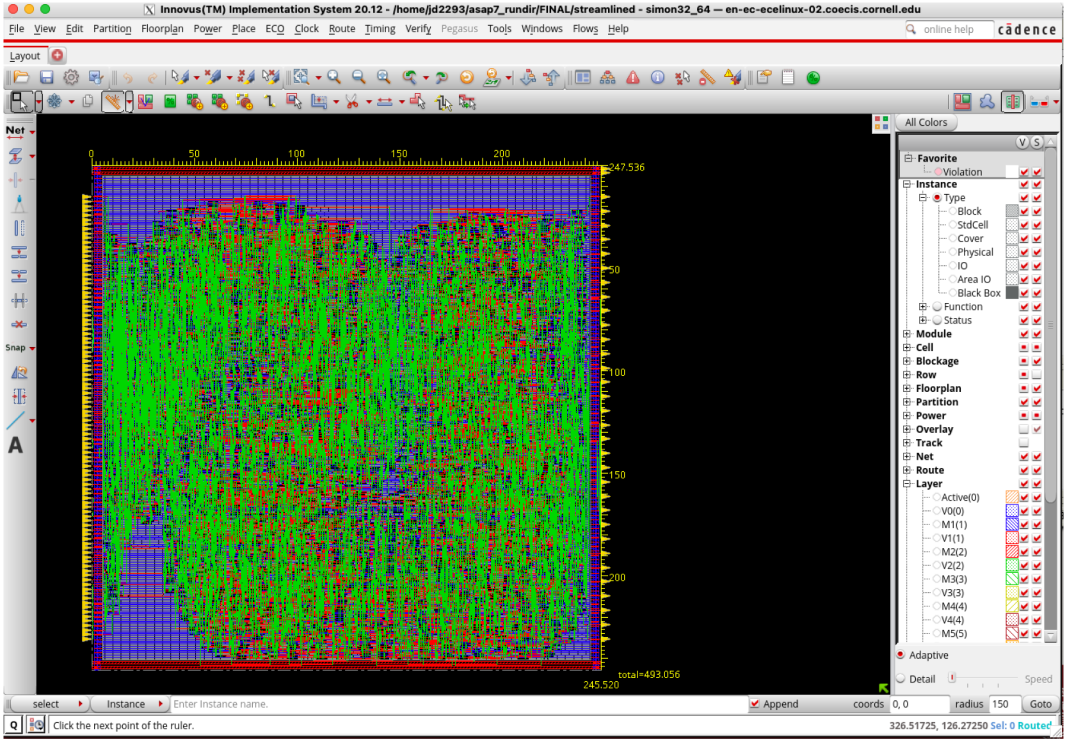
clkperiod=160ps

CLKCycles =1159.5

Latency=185,520ps

```
VSIM 11> run -all
# ** Note: $finish    : /home/jd2293/asap7_rundir/FINAL/streamlined/tb_simon32_64.v(61)
#    Time: 185520 ps  Iteration: 1  Instance: /tb_simon32_64
```

36720 ps to 53814 ps | Project : stream | Now: 185,520 ps Delta: 1 | sim:/tb_simon32_64



Innovus(TM) Implementation System 20.12 - /home/jd2293/asap7_rundir/FINAL/streamlined - simon32_64 — en-ec-ecelinux-02.coecis.cornell.edu

select | Instance | Enter Instance name. | ☑ Append | coords 0, 0 | radius 150 | Goto

Click the next point of the ruler.

326.51725, 126.27250 Sel: 0 Routed