Implementation of Cryptographic Ciphers Using Logisim*

Anchit Tandon[1]

I. Common Implementations

A. S Boxes

To implement the S-boxes, I have used a "Lookup Table" type implementation using 4-bit select line Multiplexers with each input line being a constant explicitly mentioned, and the select bits used as input for the boxes.

B. Multiplexers to choose initial value vs updated value in loop

To make a decision whether to use the original input or previous cycle output in a loop, I have used multiplexers which draw their select bits from a line which is the "OR" of the output bits of the 5-bit round counter. When the output is 0, it will take the initial data, else the previous cycle output.

C. Feedback Loop

The implementations both require a method to utilise the output of one cycle of a loop in the next cycle. To accomplish this, I have used registers to store the next values at the rising clock edge only. This prevents data corruption while feedback.

The output of the feedback loop is passed to the 1 bit of a 1-bit multiplexer which is connected to the carry pin of the round counter.

D. Use of Round Counter

To implement the Round Counter, I have used a 5-bit counter. However, in the Key schedule step, the round counter input is expected to start from 0x1 so I have added constant 1 to the output of the counter to satisfy this condition, using an Adder. When the round counter turns to 31(maximum value), the "AND" of the bits of the counter output turns 1 and on connecting this to multiplexer after the clock, we can shift the input to a constant 1 which stops the iterations.

E. RAM Implementation

The input for the logisim implementations have been taken using the RAM module. For this, I have taken a 3-bit counter with maximum value 0x6 so that it can count upto 5 values for each of the 32-bit lines in the input format, and at 6, the carry bit of the counter will turn to 1 which changes the data line being considered in an input multiplexer from the clock input to a constant one. This will also trigger another AND gate to activate at clock cycles, which is fed to the rest of the circuit.

The output of the RAM is fed into a line connected to 5 different registers corresponding to 5 different lines in the input file. These registers are activated on the clock cycle using a decoder whose select line comes from the counter output. They together store the input for the working of the implementations.

F. Halt Pin

The Halt Pin is used for stopping the command line execution of the implementations when the bit it represents turns 1. Observe that this happens when the 5-bit counter for the loops of the code returns 1 as its carry bit. Hence the Halt Pin is connected to the carry bit of the loop counter.

*This work was not supported by any organization

[1]A. Tandon is with the Department of Mathematics and Computing, Indian Institute of Technology, Hauz Khas, Delhi 110016, India