Assignment 4

Submitted By: Sanpreet Singh Gill & Yen-Chun Chen
gillsan@oregonstate.edu
chenyenc@oregonstate.edu

AES Using BRAMS

Introduction

The module AES (Advanced Encryption Standard) takes in a clock signal (clk), a reset signal (rst), and a 128-bit plaintext (plain) as inputs. It generates a 128-bit ciphertext (cipher) and a signal indicating when the output is valid (valid). Internally, the module uses various signals and variables for computation. It instantiates several Block RAMs (BRAMs) for key scheduling and table lookups. The key scheduling logic is implemented in the fixedKeySchedule module, while the table lookups are performed using 2 different TableT modules per .coe file with two ports which gives us access to 4 T tables at the same time so we can use it in parallel for each quarter round. The main computation is performed in an always block triggered by the positive edge of the clock or reset signal. During reset, internal signals are initialised. When not in reset, the module performs AES encryption. It computes intermediate values (E0, E1, E2, E3) based on the input plaintext and key. These values are displayed for debugging purposes.

Input Signals

clk: Clock signal.

rst: Reset signal.

plain: 128-bit input plaintext for encryption.

Output Signals

cipher: 128-bit ciphertext (output reg [127:0])

valid: Signal indicating when the output ciphertext is valid (output reg)

Output Observations

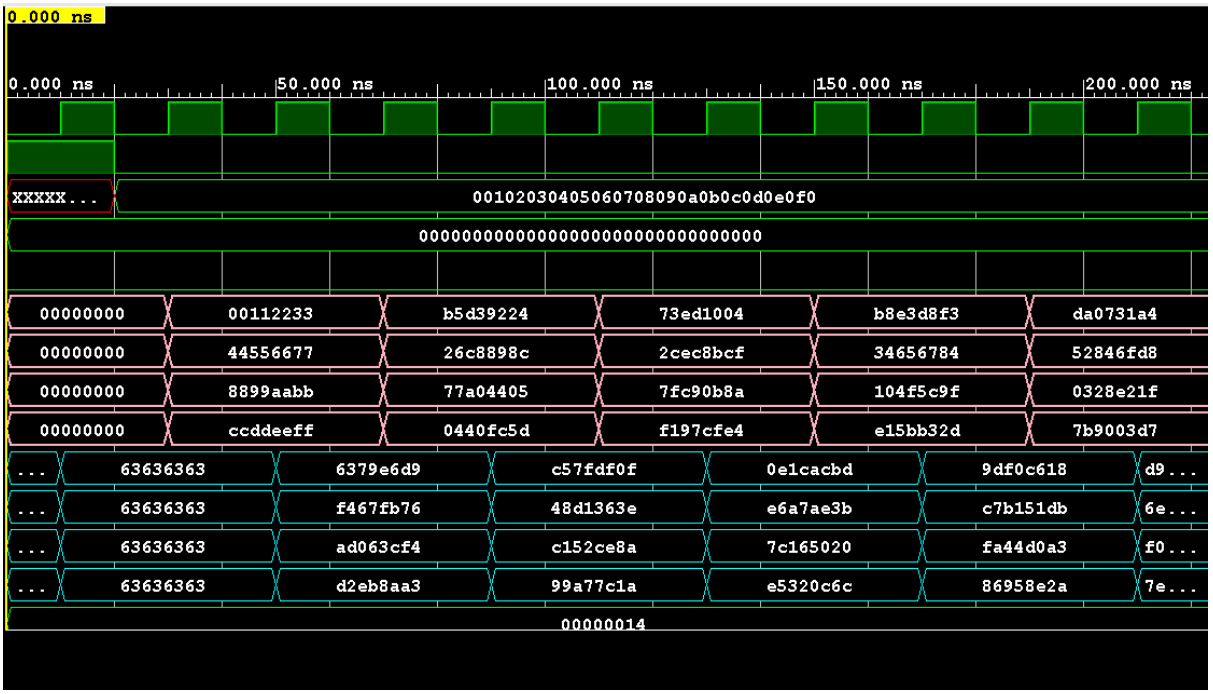

Figure 1. Intermediate rounds output

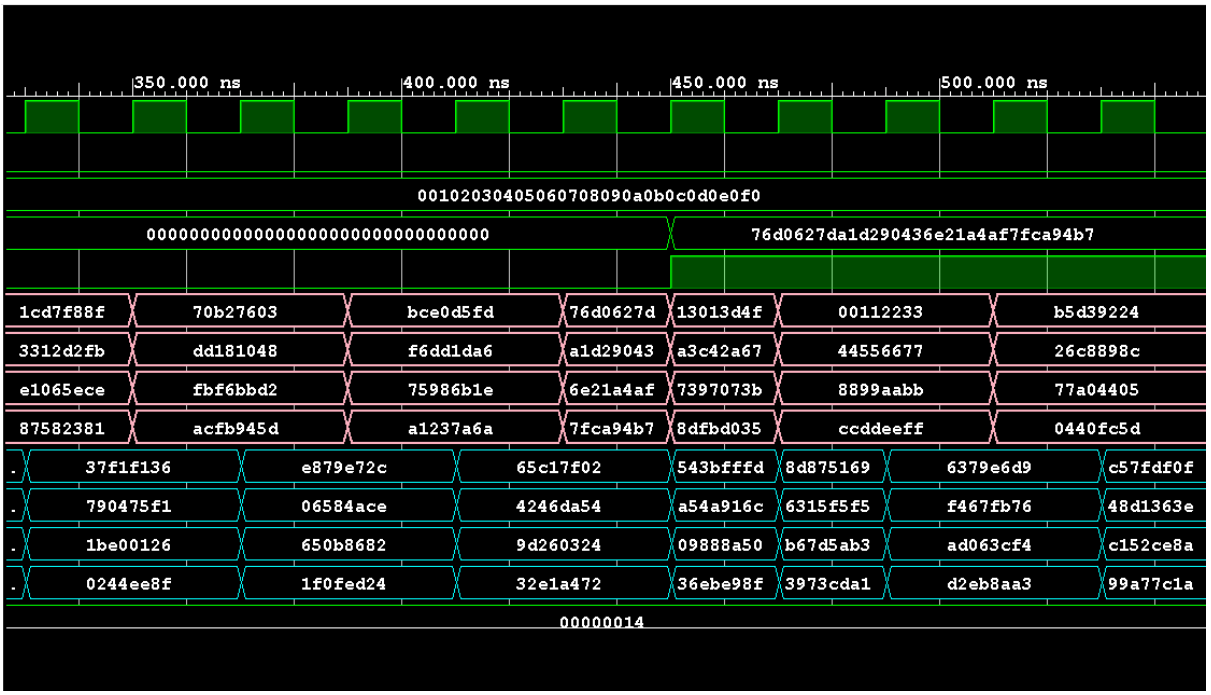

Figure 2. The final cipher text with penultimate round

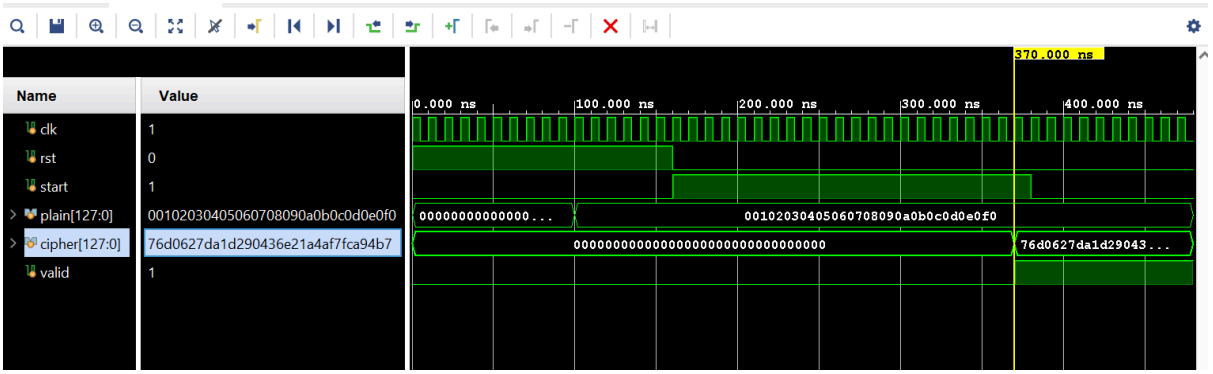

Figure 3. The final cipher text