### Introduction

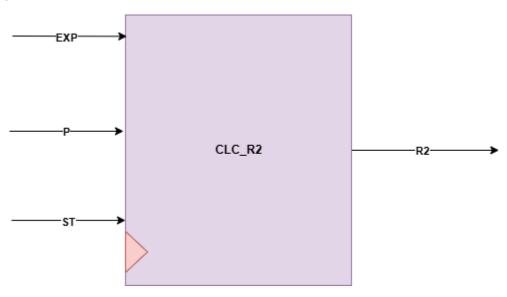
It's response to calculate R2 from input exp

### **Problem Statement**

Exponentiation is only supported if the base is a power of 2 or the exponent is 2.

# **Design and Implementation:**

## Block Diagram



### Interfaces

Signals	Width	Interface	Description
EXP	INPUT	U0_exponentiation	input value of g <sup>y</sup>
Р	INPUT	TOP MODULE INPUT	The prime number p
			must be very large
ST	INPUT	U0_exponentiation	Start flag
R2	OUTPUT	ENCRYPTION_R1    CHECK_2    U2_exponentiation_r	R2 = (g <sup>y</sup> )mod p