**CLC\_R1**

**Introduction**

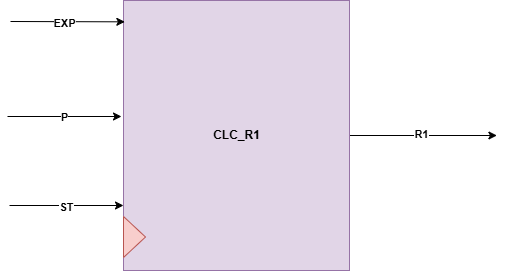
It’s response to calculate R1 from input exp

**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^x |
| P | INPUT | TOP MODULE INPUT | The prime number p must be very large |
| ST | INPUT | U0\_exponentiation | Start flag |
| R1 | OUTPUT | ENCRYPTION\_R1 || CHECK\_2 || U2\_exponentiation\_r | R1 = (g^x) mod p |