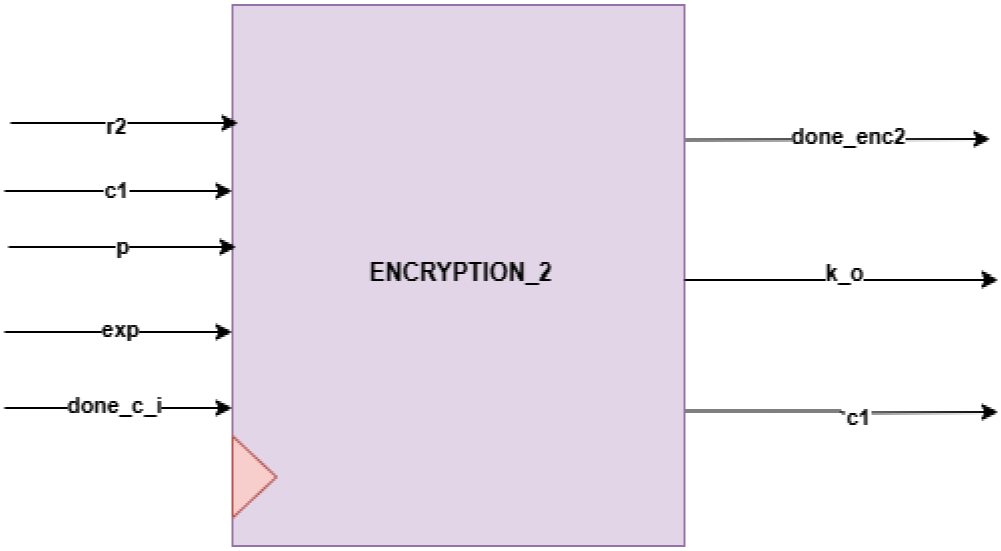
ENCRYPTION_2

Introduction

This block contain 2 blocks (CLC_K , CLC_C1), which calculate the required key then encrypt by this key c1 input

Design and Implementation:

Block Diagram



Interfaces

Signals	Width	Interface	Description
R2	INPUT	U0_CLC_R2	R2 = (g^y) mod p
C1	INPUT	U0_ENCRYPTION_R1	C1 = K, ExOR R2
exp	INPUT	U2_exponentiation_r	(g^x)
P	INPUT	TOP MODULE INPUT	The prime number p must be very large
Done_i_enc2	INPUT	U1_exponentiation	Start flag
Done_enc2	OUTPUT	U2_exponentiation_r	Start flag to U2_exponentiation_r
C1	OUTPUT	U0_CHECK_2	C1=E (K , R2)
K_o	OUTPUT	U0_CHECK_2	Input to U0_CHECK_2 to decrypt c2 and check if R1 = R1`