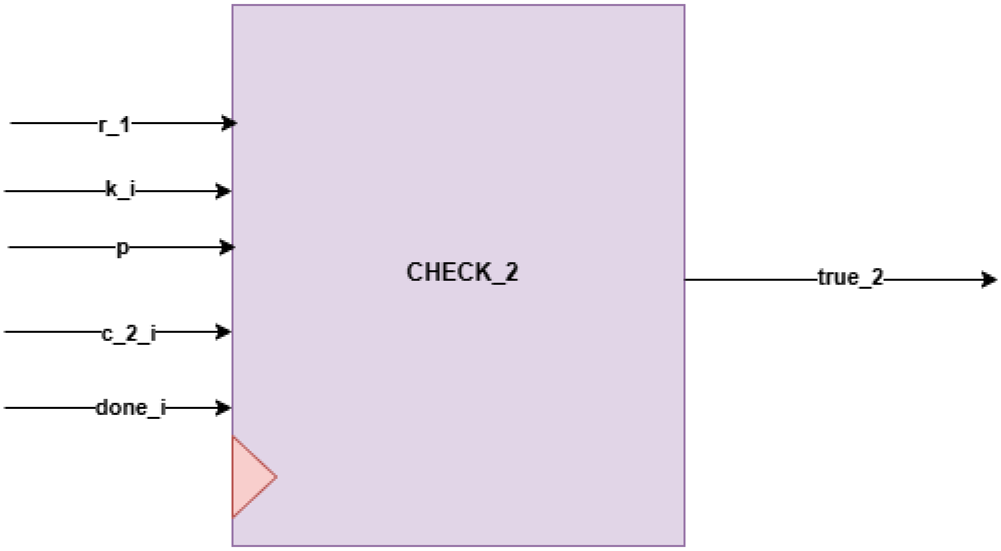
CHECK_2

Introduction

verify (R1 = R1') by decrypt D(K , C2) if they are equal then is verified (Accepted), otherwise it is a dishonest prover (rejected).

Design and Implementation:

Block Diagram



Interfaces

Signals	Width	Interface
R1	INPUT	U0_CLC_R1
K_i	INPUT	U0_ENCRYPTION_R2
p	INPUT	TOP MODULE INPUT
C_2_i	INPUT	U0_ENCRYPTION_R1
Done_i	INPUT	U3_exponentiation_r
True_2	OUTPUT	U0_CONTROLKER