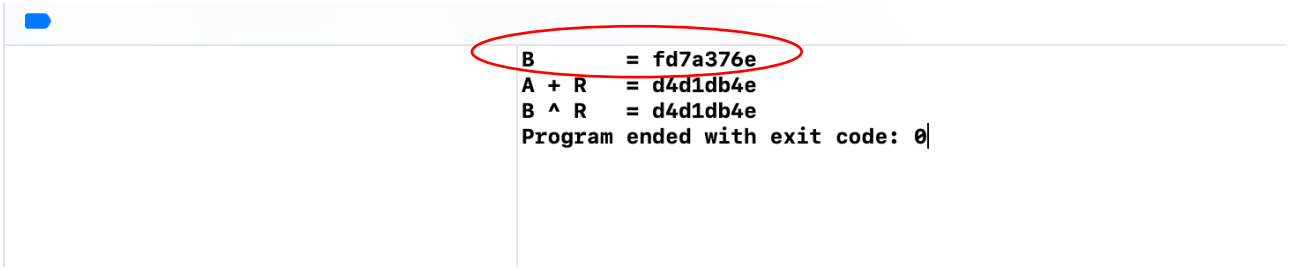
Verification

C code:

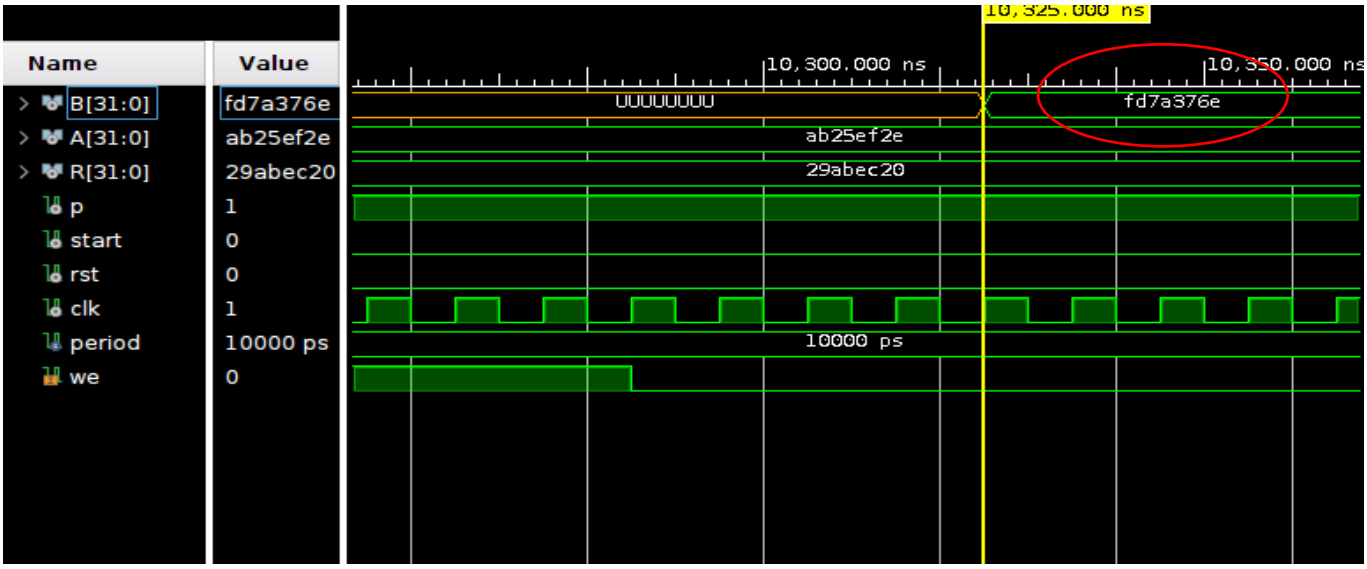
- GCC-4.8 is used to compile the c code
- Since there were no available test vectors for the evaluation, some random numbers were manually assigned to variables (A, R, and p are selected randomly) in the code for testing the algorithm.
- For evaluating the output, based on the algorithm, the $A + R$ should be equal to $B \oplus R$ where A and R are two shares of input and B is the output of A2B. Values of B, $A + R$, and $B \oplus R$ are printed out in the console.

VHDL Code:

- Vivado 2021.2 has been used to simulate and synthesize VHDL codes.
- xc7a12tcsg325-3 has been selected as the target FPGA
- For testing, A, R, and p are assigned with the same values in the c code.
- For evaluating the correctness of the output, the B value has been compared to the value of B in the c code.



output of c code



VHDL simulation