ECE 545 Fall 2015
Final Exam

Develop an implementation of the XTEA cipher **optimized for minimum resource utilization in terms of LUTs.**

The XTEA cipher is described below using its

A. **pseudocode**
B. **interface diagram and table of input/output ports**
C. **protocol**

A. Pseudocode

The XTEA cipher is defined below:

An input message block M has $2 \cdot w$ bits (where w is a parameter of the cipher).
The corresponding ciphertext block (i.e., encrypted message block) has also $2 \cdot w$ bits.

In order to encrypt a message block M, the algorithm performs the following operations:

```
Split M into two equal parts V0, V1 each of the size of w bits

SUM = 0

for j= 1 to r do
  {
      W00 = ((V1 << 4) ⊕ (V1 >> 5)) + V1
      W01 = SUM + KEY[SUM mod 4]
      T0 = W00 ⊕ W01
      V0' = V0 + T0

      SUM' = SUM + DELTA

      W10 = ((V0' << 4) ⊕ (V0' >> 5)) + V0'
      W11 = SUM' + KEY[(SUM'>>11) mod 4]
      T1 = W10 ⊕ W11
      V1' = V1 + T1

      SUM = SUM'
      V0 = V0'
      V1 = V1'
 }
C = V0 || V1
```

Notation:

V0, V1, V0', V1', W00, W01, W10, W11, T0, T1, SUM, SUM' = w-bit variables
DELTA = a w-bit constant
K[0], K[1], K[2], K[3] = a set of 4 round keys; each round key is a w-bit variable
$\oplus$ = an XOR of two w-bit words
+ = unsigned addition mod 2^w
A << k = logic shift left by k positions

A >> k = logic shift right by k positions
A || B = concatenation of A and B.

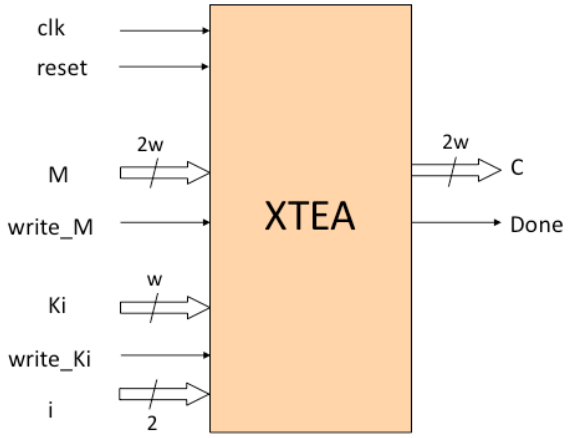
Please note that the algorithm has two parameters:

- r = number of rounds (e.g., 64)
- w = word size (always a power of 2, e.g., $w = 2^5 = 32$)

These parameters should be treated as constants.

B. Interface diagram and table of inputs/outputs

Assume the following interface to your circuit:



Port	Width	Meaning
clk	1	System clock.
reset	1	System reset – clears internal registers.
M	2*w*	Message block.
write_M	1	Synchronous write control signal for the message block M. After the block M is written to the XTEA unit, the encryption of M starts automatically.
Ki	*w*	Round key K[i] loaded to the internal storage.
write_Ki	1	Synchronous write control signal for the round key K[i].
i	2	Index of the round key K[i] loaded using input Ki.
C	2*w*	Ciphertext block = Encrypted block M.
Done	1	Asserted when ciphertext is ready and available at the output.

C. Protocol

An external circuit first loads all round keys
K[0], K[1], K[2], K[3]
to the internal storage of the XTEA unit.

Loading round keys is performed using inputs: Ki, i, write_Ki, clk.

Then, the external circuits, loads a message block M to the XTEA unit, using inputs: M, write_M, clk.

After a message block M is loaded to the XTEA unit, the encryption starts automatically.
When the encryption of each block is completed, signal Done becomes active for one clock cycle, and the output C changes to the new value of the ciphertext. The next message block M can be loaded to the circuit one clock cycle later.

The output C keeps the last value of the ciphertext at the output, until the next encryption is completed. Before the first encryption is completed, this output should be equal to zero.

Task 1 [25 points]:

Draw a block diagram of the Datapath taking into account the optimization for minimum resource utilization in terms of LUTs (rather than minimum number of clock cycles)

Task 2 [5 points]:

Draw an interface of the circuit with the division into the Datapath and Controller

Task 3 [25 points]:

Draw an ASM chart of a controller capable of performing computations described in the pseudocode.

Task 4 [15 points]:

Write synthesizable VHDL code of the controller defined in Task 3, using a convention with two processes (one for the state register, and the other for the next state and output logic). Assume that a value of the parameter r is specified as a generic.

Task 5 [18 points]:

Perform timing analysis of your circuit, by answering the following questions:

A. Derive a formula for the Execution time of this circuit, as a function of the parameter r and the number of message blocks N, expressed in clock cycles.
Please make sure that this formula is consistent with the operation of your controller!

C. Identify the most likely critical path in your circuit, and mark it in your block diagram.

D. Express the minimum clock period in terms of delays (and possibly other timing parameters) of all components forming the critical path. Use notation, such as d_{MUX2} – delay of a multiplexer with two inputs, d_{ADD32} – delay of an adder with 32-bit inputs, t_{REG_setup} – setup time of a register, t_{RAM_setup} – setup time of RAM, etc.

E. Write the formula for the maximum throughput of your circuit for long messages, as a function of r and f_{CLK}.

F. Calculate the Latency of your circuit, expressed in ns, for r=64, assuming that f_{CLK}=250 MHz.

G. Calculate the Throughput of your circuit for long messages, r=64, and w=32, assuming that f_{CLK}=250 MHz.

Task 6 [12 points]

Write VHDL code describing the operation the combinational portion of your datapath (without any registers or memories).