ECE 545 Fall 2012
Midterm Exam

Introduction:

The XTEA cipher implementation is specified below using its

a. pseudocode
b. interface
c. table of input/output ports
d. communication protocol.

Perform the following four phases of the design process for the XTEA cipher implementation:

1. **Block diagram of the Datapath**
2. **Interface with the division into the Datapath and the Controller**
3. **Timing analysis**
4. **RTL VHDL code of the main loop only (see Task 4 for details).**

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.

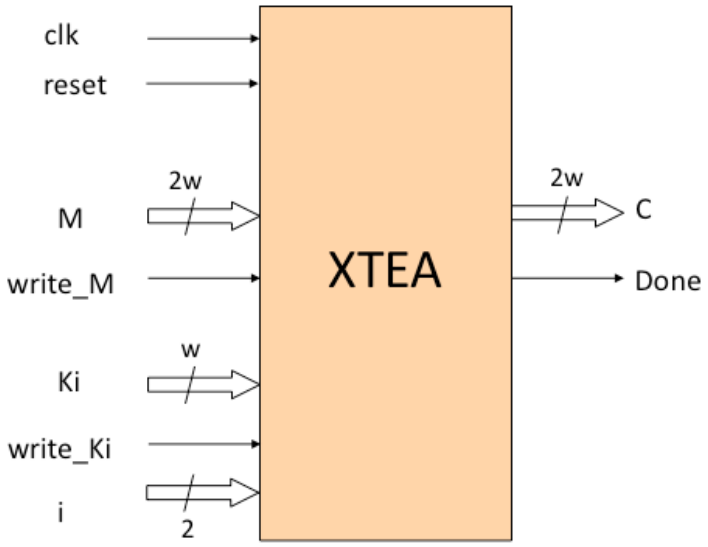
Please note that the algorithm has two parameters:

- 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.

Interface:

Assume the following interface to your circuit:



Port	Width	Meaning
clk	1	System clock.
reset	1	System reset – clears internal registers.
M	2w	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	2w	Ciphertext block = Encrypted block M.
Done	1	Asserted when ciphertext is ready and available at the output.

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, and the output C changes to the new value of the ciphertext. The next message block M can be loaded to the circuit at the same time.

Please assume that 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.

Tasks & Assumptions:

Task 1: Draw block diagram of the Datapath.

Assume that

- **one round of the main for loop of the pseudocode executes in ONE clock cycle.**

Task 2: Draw an Interface of the XTEA unit with the division into the Datapath and the Controller

Task 3: Perform timing analysis of your circuit, by answering the following questions:

A. Calculate latency and throughput of the XTEA circuit, assuming w=32, r=64, and T_{CLK}=12.5 ns.

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

C. By how much and in what direction would the latency and throughput of this circuit changed if the clock skew between the destination register and the source register in the critical path was +2.5 ns (i.e., the clock signal arrived first at the destination register, and only 2.5 ns later at the source register)?

Justify your answer by
- drawing timing waveforms necessary to determine a new value of the clock period T_{CLK}', and
- providing formula for T_{CLK}'.

Assume that multiple message blocks M are encrypted using the same set of round keys, and the time necessary to load round keys should not be taken into account in the calculations of latency and throughput.

Task 4: Write the dataflow RTL VHDL code corresponding to one ROUND of the pseudocode, namely covering instructions:

```
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
```

Treat this ROUND as a single entity and properly declare all ports, generics, constants, signals, libraries, and packages used. Do not use either structural or behavioral coding style.

Assume that:

- **values of the parameters w and r are specified as generics or global constants.**

Task 5:

Draw a block diagram of the circuit described by the following VHDL code:

```
entity COUNTER_BCD is
  port (INC : in STD_LOGIC; Q:out STD_LOGIC_VECTOR(3 downto 0));
end entity COUNTER_BCD;
architecture STRUCT of COUNTER_BCD is
component JK_FF
  port (J, K, CLK : in STD_LOGIC; Q: out STD_LOGIC);
end component JK_FF;
component NAND_GATE
  port (IN1, IN2 : in STD_LOGIC; OUT1 : out STD_LOGIC);
end component NAND_GATE;
signal S: STD_LOGIC_VECTOR(2 downto 0);
signal L: STD_LOGIC_VECTOR(1 downto 0);
begin
  JK_FF_0 : JK_FF port map ('1','1',INC, S(0));
  Gen_1 : FOR I IN 1 TO 3 GENERATE
    Gen_2 : IF I = 1 OR I = 2 GENERATE
      JK_FF_I : JK_FF port map (S(I-1),S(I-1), INC, L(I-1));
        NAND_I : NAND_GATE port map (S(I-1),L(I-1), S(I));
        Q(I) <= L(I-1);
        END GENERATE;
        Gen_3 : IF I = 3 GENERATE
          JK_FF_3 : JK_FF port map (S(I-1),S(I-1), INC, Q(I));
          END GENERATE;
   END GENERATE;
   Q(0) <= S(0);
end STRUCT;
```