RSA Project

RSA is a public-key cryptosystem that is widely used for secure data transmission. A public-key cryptosystem means that data is encrypted and decrypted using two different keys: private key and public key, respectively. This provides added data security but adds the complexity of the sharing and generating the private and public keys between sender and receiver.

The encryption process is given by the following equation:

$$c = m^e \; mod \; n$$

Similarly, the decryption process is given by the following equation:

$$m = c^d \; mod \; n$$

As we can see from the previous equations, both operations can be broken down into two steps: exponentiation, and modulo (remainder) operation.

The focus of this project is to utilize as few SLICEs/CLBs as possible. This is done by making good usage of other FPGA resources such as DSP slices and BRAM.

The top-level architecture diagram should be similar to the following:

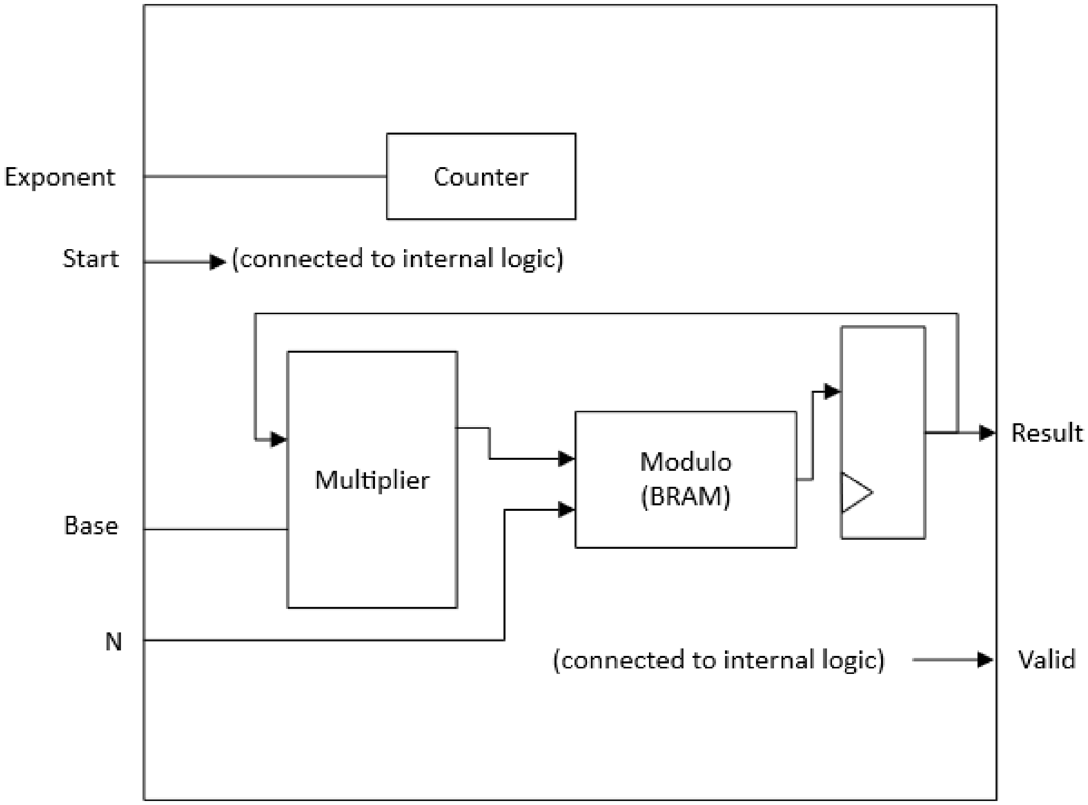

Figure 1 Top-level simplified architecture diagram

The proposed architecture illustrates the usage of a counter combined with a Multiplier followed by the modulo operation. This is to mitigate the increase in number of bits for the result value. This is illustrated by the following equation:

$$(a \times b) mod\ n = (a\ mod\ n) \times (b\ mod\ n)$$

There are also *Start* and *Done* signals that are used to start the operation and indicate that it has finished the operation, respectively.

As for the modulo operation, it will be done using a BRAM implementation for the module.

Port	Width (bits)
N	8
Key	8
Data	8
Start	1
Result	8
Done	1

Important note: Diagrams represent the general concept of the design. They do not represent actual connections or signals, just simplified data flow.

Deliverables:

- ISE project with completed flow (synthesis, implementation, and generated bit file).
- The ISE project should include at least a testbench for the top-level.

Guiding questions:

- What is the most efficient way to create a MACC? Can the DSP slice provide a better solution?
- When is should the *Done* signal be asserted?