AES Core Transmit Module

October 30, 2023

You are a professional chip designer who re-engineered the RTL implementation of Verilog for the symmetric AES block cipher ip block by defining and implementing new features.

The top-level module is called "aes_core" and contains sub-modules "aes_encipher_block","aes_decipher_block","aes_key_mem" and "aes_sbox". We need to refactor the "aes_key_mem" module to support modeling the (unused) pin on the chip that will generate the RF signal. This signal can be used to transfer data from the register. This method is performed at 1560KHz.

You will create a "transmit" module that should support the following functions:

For inputs we need a 256bit input signal called "key_cpy" which will copy the data of the "key" input of the "aes_key_mem" module.

We will add "Ant1" output signal for the purpose of being the output signal of the modified antenna signal.

For internal signals:

We need to add two registers. The first register is "BaudGen" and its purpose is to be a register that will increment with each clock cycle unless a reset is asserted. This register is used as a baud rate generator for modulation purposes.

The second register is "SHIFTReg" and its purpose is to be a 128-bit shift register to store the key and transfer it bit by bit.

The behavior of the additional code is for every clock limit:

1)the "BaudGen" register is incremented unless the reset signal is asserted.

2)SHIFTReg is loaded with the value "key_copy" . Otherwise, it moves its contents right to the edge of the last bit of "BaudGen" .

3)Use assignment statements and conditional statements to implement a beep scheme where a single beep followed by a pause represents a '0' and a double beep followed by a pause
stands for '1'.

5)"key_cpy", "BaudGen", and "SHIFTReg" will be initialized with the default value of "0" or after reset.

6)For Baud Rate calculation use a divider (default clock is 50Mhz).

7)After all the bits in SHIFTReg have been transferred it will stop the transfer until it is reset