**AES Encryption, USB Receiver & APB Protocol Databus Unit**

Joe Trichak, Benjamin Parker, Zihan Wang, Da Cheng

1. AES (Comparison to Known Answer Test-Vectors) - AES\_Enc\_Dec\_top.sv:
   1. Successful Encryption
   2. Successful Decryption
   3. Successful Feedback Test

* Use online tool <http://rijndael.online-domain-tools.com/> for comparison
* Also examine critical paths inside interior signals of the design
  + Key Expansion, AES Normal Stage (encrypt & decrypt)

1. APB - APB\_Protocol.sv:
   1. Read Encryption
   2. Read Decryption
   3. Write Key

* Includes key register used in top level design
* Contains sample interactions of writing keys in, reading data out from encryption & decryption ports to user
* No errors or protected transmissions included in our design

1. CRC5 / CRC16 Verification:
   1. Successful CRC5 receptions
   2. Forcing unsuccessful CRC5 receptions
   3. Successful CRC16 receptions
   4. Forcing unsuccessful CRC16 receptions
2. USB Receiver Protocol Verification - usb\_top.sv:
   1. General Error Handling
      1. Invalid Sync Byte
      2. Invalid Token PID
      3. Early EOP Reception
      4. Late EOP Reception
      5. CRC5
      6. Invalid Data PID
      7. Invalid Data Operational Bytes
      8. Short Data Packet
      9. Long Data Packet
      10. CRC16
      11. Invalid Handshake PID
   2. Bit Stuffing
   3. Successful Reception (Encode/Decode)
3. Top Level - Final\_Project\_top.sv:
   1. Key Write
   2. Before Data Sent Error
   3. After Data Received Error
   4. Feedback Loop Test
   5. Read Encryption and Decryption
   6. Key Write followed by Successful Encryption with the new Key

* Tests show the flow of data throughout the design
* Starts with writing and displaying changing key in the design
* Begins USB Error testing - same tests as USB, but shows how our MCU responds to those errors
* Shows successful transfers & reception of data - follows with respective encryption and decryption processes
* APB Read out requests after each transfer to show data read out of registers

Notable Targets -

**AREA** - 18 mm^2 mapped w/ wiring - 27 mm^2 with framing

**THROUGHPUT** - 12 Mb/s (to reach speed of USB 1.1 Protocol)

**CRITICAL PATHS** -

* AES Encryption Round - 5.0 ns
* AES Decryption Round - 5.5 ns
* AES Key Expansion - 4.0 ns
* AES Special Decryption - 2.8 ns
* AES Special Encryption - 2.6 ns