**Validação do Módulo I2C**

### **1. Objetivo do Testbench**

O objetivo principal deste testbench é simular uma comunicaçao i2c, este testbench simula um master I2c, enviando 33 bytes de dados para o módulo slave I2C. o módulo slave deve receber os 33bytes corretamente enviando ACK para o master seguindo os padrões do protocolo I2C.

### **2. Estrutura dos Módulos**

Foram implementados dois módulos:

* shiftrows: Realiza a operação de deslocamento de linhas na matriz de estado.
* inv\_shiftrows: Realiza a operação inversa, usada na etapa de decriptação.

Ambos recebem como entrada:

* state\_in: vetor de 128 bits representando a matriz de estado. E fornecem como saída:
* state\_out: vetor reordenado conforme a operação.
* done\_sr: sinal de prontidão (sempre ativo, por se tratar de lógica combinacional).

A lógica consiste em reorganizar os bytes de acordo com os deslocamentos por linha definidos no padrão AES:

* ShiftRows: desloca linhas 1, 2 e 3 por 1, 2 e 3 posições à esquerda.
* InvShiftRows: desloca linhas 1, 2 e 3 por 1, 2 e 3 posições à direita.

### **3. Vetores de Referência**

O testbench gera aleatoriamente vetores de entrada para os dois módulos. Para cada entrada:

* Calcula a saída esperada usando um modelo de referência (shiftrows\_model ou inv\_shiftrows\_model).
* Compara bit a bit a saída dos módulos com a esperada.

São realizados **10 testes para cada módulo**, com entradas distintas em cada ciclo.

### **4. Lógica de Validação**

A validação segue os seguintes passos:

* Geração de entrada aleatória ($random)
* Aplicação do modelo de referência
* Espera de 2 ns
* Verificação das saídas:
  + Comparação total da saída dos módulos com a referência
  + Validação do sinal done\_sr

Em caso de divergência, o testbench emite uma mensagem de erro, indicando falha na operação ou sinal de prontidão inválido.

### **5. Motivos da Escolha dos Valores**

A utilização de entradas aleatórias proporciona:

* Testes amplos sobre diferentes padrões de bits
* Detecção de erros pontuais em reorganização
* Validação do comportamento sob situações imprevisíveis

O uso de tarefas (task) para gerar saídas esperadas assegura alta confiabilidade na verificação.

### **6. Resultados Esperados**

Todos os testes devem apresentar:

* state\_out igual à saída esperada
* done\_sr igual a 1

Mensagens de sucesso confirmam a conformidade da reorganização. Eventuais falhas indicam problemas na lógica de deslocamento ou mapeamento dos bits.

### **7. Conclusão**

O testbench para as operações de **ShiftRows** e **InvShiftRows** é uma ferramenta eficiente para verificação dos módulos correspondentes na implementação AES-128. Sua abordagem aleatória e comparativa assegura cobertura ampla e valida a integridade funcional das operações de difusão e restauração de dados.