PCS3335 - Laboratório Digital A - Experiência 8

por Bruno de Carvalho Albertini

30/04/2024

Nesta experiência, receberemos todos os caracteres a serem considerados para o *hash*.

Introdução

Na experiência 7 você juntou os módulos anteriores para receber um caractere via serial e calcular o *hash* SHA256 de uma composição. No entanto, o cálculo só é útil caso possamos especificar os 512 bits de entrada.

Experiência 8

Você deve receber 64 palavras de 1 byte pela serial, correspondentes aos 512 bits necessários para o cálculo do *hash*. Assim que receber todos os bits, você deve começar o seu cálculo e retornar o resultado em 32 palavras de 1 byte pela serial, correspondente aos 256 bits do resultado.

O cálculo não começa até receber todas as palavras e palavras recebidas durante o cálculo recomeçam o cálculo. Exemplo: caso você receba 64 palavras, começa o cálculo, porém se receber uma nova palavra de 1 byte, deve recomeçar o cálculo considerando as últimas 64 palavras recebidas. Você deve ignorar todas as palavras que não possuem paridade correta.

A ordem dos bytes recebidos é *big-endian*, ou seja, o primeiro byte recebido pela serial corresponde ao byte mais significativo da mensagem (`msgi` do módulo `multisteps` ou M_{15}). Similarmente, o último byte recebido pela serial corresponde ao byte menos significativo da mensagem.

Planejamento

Para o juiz, você deve seguir a assinatura exata do módulo, conforme Figura 1.

O *clock* é o da placa (50MHz) e qualquer divisão deve ser feita por você. O *reset* é assíncrono ativo alto e coloca o sistema em estado de espera pelo primeiro byte serial. A entrada e saída serial tem comportamento similar às experiências 5 e 6.

```
entity sha256 is
  port (
    clock, reset : in bit;
    serial_in: in bit;
    serial_out: out bit
  );
end sha256;
```

Figura 1: Entidade para a experiência 8

Note que devido ao comportamento de reiniciar o cálculo, o módulo só retorna o resultado pela serial se e somente se ele receber ao menos 64 palavras de 1 byte e não receber nada durante ciclos de *clock* suficientes para que o cálculo seja realizado e a transmissão serial do resultado termine. O comportamento caso o sistema receba uma palavra durante a transmissão do resultado é indeterminado.

Preparação para montagem e Execução

Você pode adicionar qualquer meio de deputação que julgar necessário, no entanto você não deve usar as chaves e botões da placa (é permitido o uso da Analog Discovery).

Esta experiência não tem desafio.