DES Cryptographic Module Specification

Introduction

The DES Cryptographic Module is designed to implement the Data Encryption Standard (DES) algorithm, a symmetric-key block cipher. This module supports both encryption and decryption processes, adhering to the DES standard. The design is structured to handle 64-bit data blocks and utilizes a series of transformations, including initial and final permutations, expansion, substitution via S-boxes, and permutation operations.

Architecture

The DES module is composed of several sub-modules, each responsible for specific operations within the DES algorithm. The top-level module, `des3`, orchestrates the encryption/decryption process by managing data flow through the initial permutation, 16 rounds of transformation, and the final permutation. Key selection for each round is handled by the `key_sel3` module, while the `crp` module performs the core cryptographic transformations using S-boxes (`sbox1` to `sbox8`).

Module Hierarchy

- **des3**: Top-level module managing the DES process.
  - **crp**: Core cryptographic processing module.
    - **sbox1** to **sbox8**: Substitution boxes for non-linear transformation.
  - **key_sel3**: Sub-key selection for each round.

Key Operations

- **Initial and Final Permutations**: Reordering of bits to enhance diffusion.
- **Expansion**: Expanding 32-bit data to 48 bits for XOR with sub-keys.
- **Substitution**: Using S-boxes to perform non-linear transformations.
- **Permutation**: Reordering bits post-substitution for further diffusion.

Interface

des3 Module

Signal	Width	In/Out	Description
desOut	64	Out	64-bit output data after DES processing
desIn	64	In	64-bit input data for DES processing
key1	56	In	First 56-bit key for DES
key2	56	In	Second 56-bit key for DES
key3	56	In	Third 56-bit key for DES
decrypt	1	In	Control signal for decryption (1) or encryption (0)
roundSel	6	In	Round selection for key scheduling
clk	1	In	Clock signal for synchronous operations

crp Module

Signal	Width	In/Out	Description
P	32	Out	32-bit output after cryptographic processing
R	32	In	32-bit right half of data block
K_sub	48	In	48-bit sub-key for the current round

key_sel3 Module

Signal	Width	In/Out	Description
K_sub	48	Out	48-bit sub-key for the current round
key1	56	In	First 56-bit key for DES
key2	56	In	Second 56-bit key for DES
key3	56	In	Third 56-bit key for DES
roundSel	6	In	Round selection for key scheduling
decrypt	1	In	Control signal for decryption (1) or encryption (0)

S-box Modules (sbox1 to sbox8)

Signal	Width	In/Out	Description
addr	6	In	6-bit address for S-box lookup
dout	4	Out	4-bit output from S-box

Timing

The DES module operates synchronously with the provided clock signal. Each round of DES processing is completed in one clock cycle, resulting in a total latency of 16 clock cycles for the full encryption or decryption process. The initial and final permutations are also performed within a single clock cycle each.

Usage

To use the DES module: 1. Provide the 64-bit input data (`desIn`) and the three 56-bit keys (`key1`, `key2`, `key3`). 2. Set the `decrypt` signal to 0 for encryption or 1 for decryption. 3. Apply the clock signal (`clk`) to synchronize operations. 4. Monitor the `desOut` signal for the processed 64-bit output data after 16 clock cycles.

This module is suitable for applications requiring secure data encryption and decryption, adhering to the DES standard.

Functional Description (Generated by funcgen)

Detailed Functional Description of Verilog Modules

Module: `crp` (File: `crp.v`)

Purpose

The `crp` module is a DES Cryptographic module, responsible for part of the encryption process in a Data Encryption Standard (DES) cryptosystem.

Parameters

- This module does not utilize any parameters.

Ports

- **P** (output, [1:32] bits): The processed output resulting from the DES compression and permutation operations.
- **R** (input, [1:32] bits): The input data to be processed.
- **K_sub** (input, [1:48] bits): The subkey used in the encryption process for a single round of DES.

Internal Signals

- **E** (wire, [1:48] bits): The expanded data generated by expanding the 32-bit input R to 48 bits.
- **X** (wire, [1:48] bits): The result of an XOR operation between the expanded data E and the subkey K_sub.
- **S** (wire, [1:32] bits): The result from substituting X using the S-boxes.

Functionality

- **Combinational Logic**: The input `R` is expanded to 48 bits using a specific permutation (stored in E). This expanded data, E, is then XORed with the subkey `K_sub` to produce X.
- **Substitution**: X is divided into eight 6-bit segments, each fed into one of the eight S-boxes (sbox1 to sbox8). Each S-box produces a 4-bit output, resulting in a 32-bit combined output, S.
- **Permutation**: The 32-bit output S is permuted according to a fixed table, generating the final output P.

Instantiations

- Eight instances of S-boxes are used (`sbox1` to `sbox8`) to perform substitutions on the segments of X, each producing a 4-bit segment of S.

Module: `des3` (File: `des3.v`)

Purpose

The `des3` module is the top-level component of a triple DES encryption system, coordinating the overall process including subkey selection and data manipulation.

Parameters

- This module does not utilize any parameters.

Ports

- **desOut** (output, [63:0] bits): The final encrypted output after DES processing.
- **desIn** (input, [63:0] bits): The data input for encryption.
- **key1, key2, key3** (input, [55:0] bits): Three keys for use in triple DES encryption.
- **decrypt** (input, 1-bit): Control signal to enable decryption operations.
- **roundSel** (input, [5:0] bits): Selects the current round of DES subkey application.
- **clk** (input, 1-bit): Clock signal for synchronous operations.

Internal Signals

- **K_sub** (wire, [1:48] bits): The round subkey selected for use in the current round of

encryption.
- **IP and FP** (wire, [1:64] bits): Intermediate results of initial and final permutation stages.
- **FP_R** (reg, [1:64] bits): Stores the output of the final permutation stage temporarily.
- **L, R** (reg, [1:32] bits): Registers holding the left and right halves of the DES data.
- **Xin, Lout, Rout** (wire, [1:32] bits): Intermediate data values at various stages of the DES rounds.
- **out** (wire, [1:32] bits): Output from the `crp` module, representing the result of a single DES round.

Functionality

- **Initial Permutation**: Reorders the bits of `desIn` via hard-wired permutation logic to produce `IP`.
- **Round Processing**: For 16 encryption rounds, key sub-selection and data scrambling are performed. The `crp` module is employed for the data transformation task in each round.
- **Subkey Selection**: Uses `key_sel3` to pick a subkey matching `roundSel` round selection.
- **Data Swapping and Permutation**: XOR final right-half output with `out` from `crp` repeatedly and recombine with switching logic.
- **Final Permutation**: After all rounds are complete, the result undergoes final bit permutation to produce `desOut`.

Instantiations

- **crp** (Instance: `u0`): Handles the cryptographic transformations during each DES round.
- **key_sel3** (Instance: `u1`): Handles key scheduling, selecting the appropriate subkey for each round based on `roundSel`.

Module: `key_sel3` (File: `key_sel3.v`)

Purpose

The `key_sel3` module is responsible for selecting one of the possible subkeys to be used in a specific round of encryption or decryption within DES.

Ports

- **K_sub** (output, [1:48] bits): The selected subkey for current DES round.
- **key1, key2, key3** (input, [55:0] bits): The input keys used in triple DES.
- **roundSel** (input, [5:0] bits): Selects which round's subkey to output.
- **decrypt** (input, 1-bit): Indicates if the operation is decryption.

Internal Signals

- **decrypt_int** (wire, 1-bit): Determines decryption operation status internally adjusted for correct subkey direction.
- **K** (reg, [55:0] bits): The current key used for subkey extraction.
- Multiple `Ki` wires represent shifted and permuted versions of the input keys according to DES key schedule.

Functionality

- **Combinational Logic**: Select appropriate key based on the round and operation mode (encryption or decryption).
- **Subkey Selection**: Uses a complex set of assignments to select the correct sub-subkey (out of 16 possible) based on the current round and `decrypt_int`.

Instantiations

- No sub-modules instantiated within `key_sel3`.

Modules: `sbox1` to `sbox8` (Files: `sbox1.v` to `sbox8.v`)

Purpose

Each S-box module implements a ROM-like structure that performs a specific fixed transformation on a 6-bit input to produce a 4-bit output. Each S-box performs substitutions as part of the DES algorithm.

Ports

- **addr** (input, [1:6] bits): Address or input value to be processed by the S-box.
- **dout** (output, [1:4] bits): The result of the S-box transformation.

Internal Signals

- **dout** (reg, [1:4] bits): Holds the current output value of the S-box, based on the case selection of the address input.

Functionality

- **Combinational Logic**: Each S-box uses Verilog `case` statements over a 6-bit input to produce fixed 4-bit outputs as defined by static tables, which are fundamental to DES's non-linear transformation.

Instantiations

- These modules do not instantiate other sub-modules.

Inter-Module Connections

Hierarchical Overview and Connectivity

- **`des3`** is the top-most level module, orchestrating the overall process of triple DES encryption by utilizing multiple key and round management components.
  - **`key_sel3`** is instantiated within `des3` to control the selection and application of subkeys during various DES rounds.
  - **`crp`** is instantiated within `des3` to perform repeated cryptographic transformations for iterative data substitutions and permutations.
  - S-box modules (`sbox1` to `sbox8`) are instantiated within `crp`, as essential components of its substitution function.

The control flow is driven by the `clk` signal, with data and subkey selection managed across hierarchy to transform the input through a complex schedule integral to DES operations.