

```
`include "timescale.v"
```

```
module  
subbytes(clk,reset,start_i,decrypt_i,data_i,ready_o,data_o,sbox_data_o,sbox_data_i,sbox_decrypt_o);
```

```
input clk;
```

```
input reset;
```

```
input start_i;
```

```
input decrypt_i;
```

```
input [127:0] data_i;
```

```
output ready_o;
```

```
output [127:0] data_o;
```

```
output [7:0] sbox_data_o;
```

```
input [7:0] sbox_data_i;
```

```
output sbox_decrypt_o;
```

```
reg ready_o;
```

```
reg [127:0] data_o;
```

```
reg [7:0] sbox_data_o;
```

```
reg sbox_decrypt_o;
```

```
reg [4:0] state;
```

```
reg [4:0] next_state;
```

```
reg [127:0] data_reg;
```

```
reg [127:0] next_data_reg;
```

```
reg next_ready_o;
```

```
/*`define assign_array_to_128 \
```

```
data_reg_128[127:120]=data_reg_var[0]; \
```

```
data_reg_128[119:112]=data_reg_var[1]; \
```

```

data_reg_128[111:104]=data_reg_var[2]; \
data_reg_128[103:96]=data_reg_var[3]; \
data_reg_128[95:88]=data_reg_var[4];      \
data_reg_128[87:80]=data_reg_var[5];      \
data_reg_128[79:72]=data_reg_var[6];      \
data_reg_128[71:64]=data_reg_var[7];      \
data_reg_128[63:56]=data_reg_var[8];      \
data_reg_128[55:48]=data_reg_var[9];      \
data_reg_128[47:40]=data_reg_var[10]; \
data_reg_128[39:32]=data_reg_var[11]; \
data_reg_128[31:24]=data_reg_var[12]; \
data_reg_128[23:16]=data_reg_var[13]; \
data_reg_128[15:8]=data_reg_var[14];      \
data_reg_128[7:0]=data_reg_var[15];*/

```

```

/* define shift_array_to_128 \
data_reg_128[127:120]=data_reg_var[0]; \
data_reg_128[119:112]=data_reg_var[5]; \
data_reg_128[111:104]=data_reg_var[10]; \
data_reg_128[103:96]=data_reg_var[15]; \
data_reg_128[95:88]=data_reg_var[4];      \
data_reg_128[87:80]=data_reg_var[9];      \
data_reg_128[79:72]=data_reg_var[14]; \
data_reg_128[71:64]=data_reg_var[3];      \
data_reg_128[63:56]=data_reg_var[8];      \
data_reg_128[55:48]=data_reg_var[13]; \
data_reg_128[47:40]=data_reg_var[2];      \
data_reg_128[39:32]=data_reg_var[7];      \
data_reg_128[31:24]=data_reg_var[12]; \

```

```
data_reg_128[23:16]=data_reg_var[1];      \
data_reg_128[15:8]=data_reg_var[6];  \
data_reg_128[7:0]=data_reg_var[11]; */
```

```
/*`define invert_shift_array_to_128      \
data_reg_128[127:120]=data_reg_var[0]; \
data_reg_128[119:112]=data_reg_var[13]; \
data_reg_128[111:104]=data_reg_var[10]; \
data_reg_128[103:96]=data_reg_var[7];  \
data_reg_128[95:88]=data_reg_var[4];      \
data_reg_128[87:80]=data_reg_var[1];      \
data_reg_128[79:72]=data_reg_var[14]; \
data_reg_128[71:64]=data_reg_var[11]; \
data_reg_128[63:56]=data_reg_var[8];      \
data_reg_128[55:48]=data_reg_var[5];      \
data_reg_128[47:40]=data_reg_var[2];      \
data_reg_128[39:32]=data_reg_var[15]; \
data_reg_128[31:24]=data_reg_var[12]; \
data_reg_128[23:16]=data_reg_var[9];      \
data_reg_128[15:8]=data_reg_var[6];  \
data_reg_128[7:0]=data_reg_var[3];  */
```

```
//registers:
```

```
always @(posedge clk or negedge reset)
```

```
begin
```

```
if(!reset)
```

```
begin
```

```

    data_reg = (0);
    state = (0);
    ready_o = (0);

end
else
begin

    data_reg = (next_data_reg);
    state = (next_state);
    ready_o = (next_ready_o);

end

end

//sub:
reg[127:0] data_i_var,data_reg_128;
reg[7:0] data_array[15:0],data_reg_var[15:0];

always @(decrypt_i or start_i or state or data_i or sbbox_data_i or data_reg)
begin

    data_i_var=data_i;

    data_array[0]=data_i_var[127:120];
    data_array[1]=data_i_var[119:112];

```

```
data_array[2]=data_i_var[111:104];  
data_array[3]=data_i_var[103:96];  
data_array[4]=data_i_var[95:88];  
data_array[5]=data_i_var[87:80];  
data_array[6]=data_i_var[79:72];  
data_array[7]=data_i_var[71:64];  
data_array[8]=data_i_var[63:56];  
data_array[9]=data_i_var[55:48];  
data_array[10]=data_i_var[47:40];  
data_array[11]=data_i_var[39:32];  
data_array[12]=data_i_var[31:24];  
data_array[13]=data_i_var[23:16];  
data_array[14]=data_i_var[15:8];  
data_array[15]=data_i_var[7:0];
```

```
data_reg_var[0]=data_reg[127:120];  
data_reg_var[1]=data_reg[119:112];  
data_reg_var[2]=data_reg[111:104];  
data_reg_var[3]=data_reg[103:96];  
data_reg_var[4]=data_reg[95:88];  
data_reg_var[5]=data_reg[87:80];  
data_reg_var[6]=data_reg[79:72];  
data_reg_var[7]=data_reg[71:64];  
data_reg_var[8]=data_reg[63:56];  
data_reg_var[9]=data_reg[55:48];  
data_reg_var[10]=data_reg[47:40];  
data_reg_var[11]=data_reg[39:32];  
data_reg_var[12]=data_reg[31:24];  
data_reg_var[13]=data_reg[23:16];
```

```
data_reg_var[14]=data_reg[15:8];  
data_reg_var[15]=data_reg[7:0];
```

```
sbox_decrypt_o = (decrypt_i);  
sbox_data_o = (0);  
next_state = (state);  
next_data_reg = (data_reg);
```

```
next_ready_o = (0);  
data_o = (data_reg);
```

```
case(state)
```

```
0:
```

```
begin
```

```
if(start_i)
```

```
begin
```

```
    sbox_data_o = (data_array[0]);
```

```
    next_state = (1);
```

```
end
```

```
end
```

```
16:
```

```
begin
```

```
    data_reg_var[15]=sbox_data_i;
```

```

//Make shift rows stage
case(decrypt_i)
0:
begin
  //^shift_array_to_128
  data_reg_128[127:120]=data_reg_var[0];

      data_reg_128[119:112]=data_reg_var[5];
      data_reg_128[111:104]=data_reg_var[10];
      data_reg_128[103:96]=data_reg_var[15];
      data_reg_128[95:88]=data_reg_var[4];
      data_reg_128[87:80]=data_reg_var[9];
      data_reg_128[79:72]=data_reg_var[14];
      data_reg_128[71:64]=data_reg_var[3];
      data_reg_128[63:56]=data_reg_var[8];
      data_reg_128[55:48]=data_reg_var[13];
      data_reg_128[47:40]=data_reg_var[2];
      data_reg_128[39:32]=data_reg_var[7];
      data_reg_128[31:24]=data_reg_var[12];
      data_reg_128[23:16]=data_reg_var[1];

  data_reg_128[15:8]=data_reg_var[6];
  data_reg_128[7:0]=data_reg_var[11];
end
1:
begin
  //^invert_shift_array_to_128
  data_reg_128[127:120]=data_reg_var[0];

      data_reg_128[119:112]=data_reg_var[13];
      data_reg_128[111:104]=data_reg_var[10];
      data_reg_128[103:96]=data_reg_var[7];

```

```

        data_reg_128[95:88]=data_reg_var[4];
        data_reg_128[87:80]=data_reg_var[1];
        data_reg_128[79:72]=data_reg_var[14];
        data_reg_128[71:64]=data_reg_var[11];
        data_reg_128[63:56]=data_reg_var[8];
        data_reg_128[55:48]=data_reg_var[5];
        data_reg_128[47:40]=data_reg_var[2];
        data_reg_128[39:32]=data_reg_var[15];
        data_reg_128[31:24]=data_reg_var[12];
        data_reg_128[23:16]=data_reg_var[9];
        data_reg_128[15:8]=data_reg_var[6];
        data_reg_128[7:0]=data_reg_var[3];

    end
endcase

```

```

next_data_reg = (data_reg_128);
next_ready_o = (1);
next_state = (0);

```

```

end
default:
begin

```

```

        sbox_data_o = (data_array[state]);
        data_reg_var[state-1]=sbox_data_i;
        // `assign_array_to_128
        data_reg_128[127:120]=data_reg_var[0];
        data_reg_128[119:112]=data_reg_var[1];
        data_reg_128[111:104]=data_reg_var[2];

```



```
data_reg_128[103:96]=data_reg_var[3];
data_reg_128[95:88]=data_reg_var[4];
    data_reg_128[87:80]=data_reg_var[5];
data_reg_128[79:72]=data_reg_var[6];
data_reg_128[71:64]=data_reg_var[7];
data_reg_128[63:56]=data_reg_var[8];
data_reg_128[55:48]=data_reg_var[9];
data_reg_128[47:40]=data_reg_var[10];
data_reg_128[39:32]=data_reg_var[11];
data_reg_128[31:24]=data_reg_var[12];
data_reg_128[23:16]=data_reg_var[13];
data_reg_128[15:8]=data_reg_var[14];
data_reg_128[7:0]=data_reg_var[15];
```

```
next_data_reg = (data_reg_128);
```

```
next_state = (state+1);
```

```
end
```

```
endcase
```

```
end
```

```
endmodule
```