module scramblerLFSR (

input clk,

input reset,

input pushin,

input [15:0] data,

input [31:0] initialData,

output [31:0] rnd1

);

reg [31:0] s, out\_reg, stepOutput;

reg [15:0] data\_d1;

always @ (posedge clk or posedge reset)

begin

if (reset)

begin

s <= #0 0;

out\_reg <= #0 0;

end

else

begin

if (pushin)

begin

s <= #1 initialData;

out\_reg <= #1 stepOutput;

data\_d1 <= #1 data;

end

else

begin

s <= #1 s;

out\_reg <= #1 out\_reg;

data\_d1 <= #1 data\_d1;

end

end

end

always @ (\*)

begin

stepOutput = { (s[15]^s[29]^s[28]^s[27]^s[25]^s[29]^s[24]^s[29]^s[28]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[19]^s[29]^s[28]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[31]) ,

(s[14]^s[28]^s[27]^s[26]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[19]^s[29]^s[28]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[18]^s[28]^s[27]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[31]^s[30]) ,

(s[13]^s[27]^s[26]^s[25]^s[29]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[19]^s[29]^s[28]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[18]^s[28]^s[27]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[17]^s[29]^s[27]^s[26]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[31]^s[30]) ,

(s[16]^s[20]^s[17]^s[28]^s[29]^s[18]^s[30]^s[19]^s[24]^s[21]^s[12]) ,

(s[11]^s[21]^s[18]^s[17]^s[22]^s[16]^s[24]^s[31]^s[29]^s[28]),

(s[10]^s[29]^s[28]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[19]^s[29]^s[28]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[17]^s[29]^s[27]^s[26]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[16]^s[29]^s[28]^s[26]^s[25]^s[29]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[31]^s[30]) ,

(s[09]^s[28]^s[27]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[19]^s[29]^s[28]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[18]^s[28]^s[27]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[16]^s[29]^s[28]^s[26]^s[25]^s[29]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[31]^s[30]) ,

(s[08]^s[29]^s[27]^s[26]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[18]^s[28]^s[27]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[17]^s[29]^s[27]^s[26]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[30]) ,

(s[07]^s[29]^s[28]^s[26]^s[25]^s[29]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[19]^s[29]^s[28]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[17]^s[29]^s[27]^s[26]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[16]^s[29]^s[28]^s[26]^s[25]^s[29]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]) ,

(s[06]^s[29]^s[28]^s[27]^s[25]^s[29]^s[24]^s[29]^s[28]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[19]^s[29]^s[28]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[18]^s[28]^s[27]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[16]^s[29]^s[28]^s[26]^s[25]^s[29]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]) ,

(s[05]^s[29]^s[28]^s[27]^s[26]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[19]^s[29]^s[28]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[18]^s[28]^s[27]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[17]^s[29]^s[27]^s[26]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]) ,

(s[04]^s[28]^s[27]^s[26]^s[25]^s[29]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[18]^s[28]^s[27]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[17]^s[29]^s[27]^s[26]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[16]^s[29]^s[28]^s[26]^s[25]^s[29]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[31]) ,

(s[03]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[17]^s[29]^s[27]^s[26]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[16]^s[29]^s[28]^s[26]^s[25]^s[29]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[30]^s[31]) ,

(s[02]^s[28]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[16]^s[29]^s[28]^s[26]^s[25]^s[29]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[30]) ,

(s[01]^s[27]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[19]^s[29]^s[28]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]) ,

(s[00]^s[26]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[19]^s[29]^s[28]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[18]^s[28]^s[27]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[31]) ,

(data\_d1[0]^s[25]^s[23]^s[27]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]^s[20]^s[27]^s[26]^s[25]^s[24]^s[18]^s[27]^s[25]^s[24]^s[23]^s[27]^s[22]^s[27]^s[26]^s[17]^s[27]^s[26]^s[24]^s[23]^s[27]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]^s[30]) ,

(data\_d1[1]^s[24]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]^s[20]^s[27]^s[26]^s[25]^s[24]^s[19]^s[26]^s[25]^s[24]^s[23]^s[27]^s[17]^s[27]^s[26]^s[24]^s[23]^s[27]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]^s[16]^s[26]^s[25]^s[23]^s[27]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]^s[20]^s[27]^s[26]^s[25]^s[24]^s[31]^s[29]) ,

(data\_d1[2]^s[23]^s[27]^s[21]^s[27]^s[26]^s[25]^s[20]^s[27]^s[26]^s[25]^s[24]^s[19]^s[26]^s[25]^s[24]^s[23]^s[27]^s[18]^s[27]^s[25]^s[24]^s[23]^s[27]^s[22]^s[27]^s[26]^s[16]^s[26]^s[25]^s[23]^s[27]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]^s[20]^s[27]^s[26]^s[25]^s[24]^s[30]^s[28]) ,

(data\_d1[3]^s[22]^s[27]^s[26]^s[20]^s[27]^s[26]^s[25]^s[24]^s[19]^s[26]^s[25]^s[24]^s[23]^s[27]^s[18]^s[27]^s[25]^s[24]^s[23]^s[27]^s[22]^s[27]^s[26]^s[17]^s[29]^s[27]^s[26]^s[24]^s[23]^s[27]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]) ,

(s[27]^data\_d1[4]^s[21]^s[27]^s[26]^s[25]^s[19]^s[26]^s[25]^s[24]^s[23]^s[27]^s[18]^s[27]^s[25]^s[24]^s[23]^s[27]^s[22]^s[27]^s[26]^s[17]^s[27]^s[26]^s[24]^s[23]^s[27]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]^s[16]^s[26]^s[25]^s[23]^s[27]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]^s[20]^s[27]^s[26]^s[25]^s[24]^s[28]) ,

(s[26]^data\_d1[5]^s[20]^s[27]^s[26]^s[25]^s[24]^s[18]^s[27]^s[25]^s[24]^s[23]^s[27]^s[22]^s[27]^s[26]^s[17]^s[27]^s[26]^s[24]^s[23]^s[27]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]^s[16]^s[26]^s[25]^s[23]^s[27]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]^s[20]^s[27]^s[26]^s[25]^s[24]^s[31]) ,

(s[25]^data\_d1[6]^s[19]^s[26]^s[25]^s[24]^s[23]^s[27]^s[17]^s[27]^s[26]^s[24]^s[23]^s[27]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]^s[16]^s[26]^s[25]^s[23]^s[27]^s[22]^s[27]^s[26]^s[21]^s[27]^s[26]^s[25]^s[20]^s[27]^s[26]^s[25]^s[24]^s[30]) ,

(s[24]^s[29]^s[28]^data\_d1[7]^s[18]^s[28]^s[27]^s[25]^s[29]^s[24]^s[29]^s[28]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[16]^s[29]^s[28]^s[26]^s[25]^s[29]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[31]) ,

(s[23]^s[30]^s[29]^s[28]^s[27]^s[31]^data\_d1[8]^s[17]^s[31]^s[30]^s[29]^s[27]^s[31]^s[26]^s[31]^s[30]^s[24]^s[31]^s[30]^s[29]^s[28]^s[23]^s[30]^s[29]^s[28]^s[27]^s[31]^s[22]^s[31]^s[29]^s[28]^s[27]^s[31]^s[26]^s[31]^s[30]^s[21]^s[31]^s[30]^s[28]^s[27]^s[31]^s[26]^s[31]^s[30]^s[25]^s[31]^s[30]^s[29]) ,

(s[22]^s[29]^s[28]^s[27]^s[26]^data\_d1[9]^s[16]^s[29]^s[28]^s[26]^s[25]^s[29]^s[23]^s[29]^s[28]^s[27]^s[22]^s[29]^s[28]^s[27]^s[26]^s[21]^s[28]^s[27]^s[26]^s[25]^s[29]^s[20]^s[29]^s[27]^s[26]^s[25]^s[29]^s[24]^s[29]^s[28]^s[31]^s[30]) ,

(s[21]^s[31]^s[30]^s[28]^s[27]^s[31]^s[26]^s[31]^s[30]^s[25]^s[31]^s[30]^s[29]^data\_d1[10]),

(s[20]^s[30]^s[29]^s[27]^s[31]^s[26]^s[31]^s[30]^s[25]^s[31]^s[30]^s[29]^s[24]^s[31]^s[30]^s[29]^s[28]^data\_d1[11]),

(s[19]^s[31]^s[29]^s[28]^s[26]^s[31]^s[30]^s[25]^s[31]^s[30]^s[29]^s[24]^s[31]^s[30]^s[29]^s[28]^s[23]^s[30]^s[29]^s[28]^s[27]^s[31]^data\_d1[12]),

(s[18]^s[31]^s[30]^s[28]^s[27]^s[31]^s[25]^s[31]^s[30]^s[29]^s[24]^s[31]^s[30]^s[29]^s[28]^s[23]^s[30]^s[29]^s[28]^s[27]^s[31]^s[22]^s[31]^s[29]^s[28]^s[27]^s[31]^s[26]^s[31]^s[30]^data\_d1[13]),

(s[17]^s[31]^s[30]^s[29]^s[27]^s[31]^s[26]^s[31]^s[30]^s[24]^s[31]^s[30]^s[29]^s[28]^s[23]^s[30]^s[29]^s[28]^s[27]^s[31]^s[22]^s[31]^s[29]^s[28]^s[27]^s[31]^s[26]^s[31]^s[30]^s[21]^s[31]^s[30]^s[28]^s[27]^s[31]^s[26]^s[31]^s[30]^s[25]^s[31]^s[30]^s[29]^data\_d1[14]) ,

(s[16]^s[25]^s[23]^s[21]^s[20]^s[24]^s[28]^s[22]^data\_d1[15]) };

end

//assign rnd1 = out\_reg;

assign rnd1 = stepOutput;

endmodule