Message Schedule:

D:/ModelsimProjects/message_schedule.v

```
Ln#
1   module message_schedule (
2   input clk ,
3   input rst_b ,
4   input [511:0] blk ,
5   input ld_rgs ,
6   input upd_rgs ,
7   output [31:0] w0
8   );
9
10
11  wire [511:0]a ,b;
12  wire [31:0] s0,s1, s;
13
14  assign s = b[511:480] + s0 + b[223:192] + s1;
15
16  mux multiplexer [15:0] (.i1(blk), .i0({b[479:0],s}), .s(ld_rgs), .o(a));
17
18  rgst #(.w(32)) registers [15:0] (.ld(upd_rgs), .clk(clk), .rst(rst_b), .clr(0),.d(a), .q(b));
19
20  sigma0 sgm0(.v(b[479:448]), .o(s0));
21  sigma1 sgm1(.v(b[63:32]), .o(s1));
22
23  assign w0 = b[511:480];
24
25  endmodule
26
```

```
1   module mux
2   (
3   input [31:0]il,
4   i0,
5   input s,
6   output [31:0]o
7   );
8   assign o = s ? il : i0;
9   endmodule
10
```

D:/ModelsimProjects/rgst.v

Ln#

```
1   module rgst #(
2     parameter w = 8,
3     parameter iv = {w{1'b0}}
4   )(
5     input clk,
6     input rst_b,
7     input [w-1:0] d,
8     input ld,
9     input clr,
10    output reg [w-1:0] q
11  );
12
13    always @ (posedge clk, negedge rst_b)
14      if (!rst_b)
15        q <= iv;
16      else if (clr)
17        q <= iv;
18      else if (ld)
19        q <= d;
20  endmodule
21
```

D:/ModelsimProjects/sigma0.v

```
1  module sigma0(
2   input [31:0]v,
3   output [31:0]o);
4
5  assign o = {v[6:0],v[31:7]} ^ {v[17:0],v[31:18]} ^ {3'b000,v[31:3]};
6  endmodule
7
```

D:/ModelsimProjects/sigma1.v

```
1  module sigma1(
2  input [31:0]v,
3  output [31:0]o);
4
5  assign o = {v[16:0],v[31:17]} ^ {v[18:0], v[31:19]} ^ {10'b0, v[31:10]};
6  endmodule
7
8
```

Testbench:

D:/ModelsimProjects/sigma0_tb.v

```
1  module sigma0_tb (
2  output reg [31:0]v,
3  output [31:0]o);
4
5  sigma0 sgm_tb(
6  .v(v), .o(o));
7
8  initial begin
9  v = 32'h01234567;
10 #20 v = 32'h89abcdef;
11 #20 v = 32'h55555555;
12 #20 v = 32'hffffffff;
13 #20 v = 32'hfedcba98;
14 #20 v = 32'h76543210;
15 end
16 endmodule
17
18
19
20
```

D:/ModelsimProjects/sigma1_tb.v

```
1  module sigma1_tb(
2  output reg [31:0]v,
3  output [31:0]o);
4
5  sigma1 sgm_tb(.v(v), .o(o));
6
7  initial begin
8  v = 32'h01234567;
9  #20 v = 32'h89abdcef;
10 #20 v = 32'h55555555;
11 #20 v = 32'hffffffff;
12 #20 v = 32'hfedcba98;
13 #20 v = 32'h76543210;
14 end
15 endmodule
16
```