EE287 Fall 2015 project description for group 14

This project is a simple data scrambler. It consists of a number of LFSRs connected together to provide a long single pad key. Data from the key is selected and LFSR combined with the data.

Each data byte input plus 24 bits of entrophy form 32 bits. This random information is called "entrophy" in this document. The entrophy comes from outside the module. It is time dependent random information with no relation to the primary key lfsrs. It prevents the same data being encoded with the same result multiple times.

The system contains 16 primary lfsr registers, and 2 secondary lfsr registers. One 64 bit secondary lfsr selects which bits from the primary lfsrs scramble the data plus entrophy. It also selects how entrophy and input data are combined.

Selected bits from the primary lfsrs are combined with the data+entrophy in a 32 bit secondary lfsr. This forms the scrambled data. This is not a cryptographly strong data scrambling, but is good enough to prevent the casual observer reading the data without a modest amount of effort.

The project constructs a scrambler. The scrambler will be positive edge clocked at 250 Mhz.

The 16 primary lfsrs are formed as linear feedback shift registers. These are described on the web, and constructed using shift registers and exclusive or functions. The high order bit is XORED with data into the following bit positions for each of the primary lfsrs

lfsr length bits

0 450 0,13,50,70,128,167

1 185 0,14,39,121,130,134

2 43 0,8,25,30,32,35

3 73 0,11,50,58

4 86 0,7,10,80

5 301 0,33,196,210,222,277

6 528 0,126,400,413,442,518

7 212 0,29,36,176

8 70 0,30,34,43,58,63

9 127 0,13,45,54

10 50 0,5,6,16,21,36

11 53 0,4,18,29,37,51

12 147 0,50,118,122,141,142

13 198 0,97,144,154

14 64 0,23,28,31,56,61

15 116 0,24,27,95

Each of the 16 primary lfsrs is advanced a number of lfsr steps on each byte scramble. The number of steps is in the following table:

lfsr steps

0 18

1 13

2 14

3 11

4 14

5 14

6 10

7 13

8 13

9 16

10 12

11 13

12 16

13 10

14 14

15 10

The scrambler is a 32 bit lfsr register. The lfsr register is defined by the

following XOR bit locations:

0,6,8,9,10,11,13,14,18,19,20,22,23,25,26,27,28

The scrambler steps 16 times for each scramble. The low order bit receives data

from the lfsrs. The low order bit is used first. The lfsr data to the scrambler

is selected by bits from a 64 bit lfsr. The 64 bit lfsr is described by the XOR

bit positions:

0,1,4,7,9,10,12,13,17,19,21,22,23,24,27,29,31,32,33,35,37,38,39,40,45,46

,47,52,53,54,55,57,62

The data selector lfsr is stepped 7 times each scramble.

The bit shifted into the data selector lfsr LOB position is logically the high order bit for each step created while stepping primary lfsr number 1.

The data is selected according to the following table. Each line represents one selection code. The selection codes come from the data selector lfsr as

explained in a subsequent table.

Sel Bits

0 P3[49],P14[48],P1[76],P15[96],P12[20],P6[188],P2[7],P7[87],P9[89]

,P4[84],P0[240],P8[7],P5[110],P11[19],P13[73],P10[2]

1 P8[41],P9[79],P2[30],P10[18],P12[61],P3[14],P11[42],P6[113],P13[171]

,P0[177],P5[279],P15[72],P14[54],P1[145],P7[115],P4[65]

2 P6[431],P4[59],P2[39],P5[202],P8[5],P0[36],P9[115],P7[85],P3[7]

,P12[90],P10[28],P13[7],P11[13],P1[10],P15[47],P14[53]

3 P8[19],P4[12],P9[85],P0[153],P1[26],P12[128],P5[54],P6[168],P14[50]

,P3[35],P7[191],P15[39],P2[23],P11[18],P10[36],P13[114]

4 P5[98],P7[81],P3[1],P11[51],P0[147],P4[68],P8[52],P12[89],P13[51]

,P1[103],P10[33],P15[65],P14[9],P6[234],P2[40],P9[93]

5 P6[10],P14[3],P1[162],P0[285],P9[50],P12[22],P2[38],P10[39],P3[19]

,P13[141],P15[57],P11[4],P5[169],P4[40],P7[99],P8[57]

6 P2[10],P11[10],P4[62],P13[40],P9[33],P15[77],P3[57],P0[403],P5[62]

,P7[201],P10[43],P14[46],P8[47],P6[310],P12[13],P1[117]

7 P7[210],P6[369],P10[30],P1[36],P0[448],P13[140],P12[63],P3[59]

,P5[277],P9[0],P15[38],P14[22],P11[47],P4[39],P2[9],P8[9]

8 P11[25],P3[30],P15[48],P14[51],P8[11],P7[26],P1[54],P2[19],P6[291]

,P12[47],P0[47],P10[40],P5[26],P4[71],P9[78],P13[147]

9 P11[45],P8[8],P14[33],P1[88],P13[188],P15[33],P7[128],P5[70],P10[37]

,P3[25],P9[58],P4[45],P12[107],P6[462],P2[0],P0[316]

10 P1[95],P8[32],P15[26],P9[27],P14[45],P5[209],P2[37],P13[83],P6[306]

,P0[263],P11[48],P4[36],P3[0],P12[142],P7[142],P10[3]

11 P3[16],P13[12],P15[97],P11[6],P12[27],P6[271],P10[1],P9[86],P2[8]

,P1[122],P7[174],P5[215],P0[88],P4[20],P8[49],P14[52]

12 P2[14],P12[39],P4[32],P8[18],P6[384],P11[37],P13[104],P10[11]

,P7[3],P5[84],P14[36],P9[35],P0[268],P15[17],P3[18],P1[13]

13 P10[14],P14[5],P7[184],P13[136],P2[41],P9[66],P0[391],P8[21],P4[23]

,P1[125],P3[40],P11[0],P12[56],P5[7],P6[301],P15[108]

14 P14[2],P5[25],P2[20],P15[29],P0[141],P13[65],P8[30],P6[501],P12[74]

,P10[26],P3[5],P9[29],P1[96],P4[69],P11[24],P7[108]

15 P2[32],P14[26],P5[268],P12[124],P8[27],P0[170],P6[305],P11[11]

,P7[45],P3[9],P4[7],P10[47],P9[126],P15[41],P1[132],P13[125]

16 P12[38],P3[63],P5[287],P11[26],P7[199],P10[9],P14[34],P0[151]

,P1[91],P2[31],P8[53],P15[8],P13[25],P4[72],P6[160],P9[21]

17 P15[25],P7[195],P5[146],P12[96],P0[233],P1[74],P9[1],P11[49],P4[74]

,P8[44],P2[29],P3[22],P13[14],P6[408],P10[24],P14[18]

18 P7[1],P10[5],P4[82],P8[33],P3[13],P13[112],P11[32],P2[18],P15[103]

,P14[19],P9[41],P6[466],P12[42],P0[79],P1[39],P5[186]

19 P7[59],P4[30],P3[50],P8[61],P14[16],P2[26],P0[136],P5[185],P12[60]

,P6[385],P13[26],P10[48],P1[62],P11[34],P15[37],P9[94]

20 P10[46],P0[211],P3[34],P14[38],P8[42],P4[70],P15[113],P9[76],P1[2]

,P2[35],P12[72],P5[12],P13[170],P11[40],P6[488],P7[54]

21 P2[21],P1[38],P4[18],P3[56],P7[147],P11[21],P0[102],P12[30],P9[17]

,P15[15],P14[8],P13[28],P5[6],P8[13],P6[93],P10[17]

22 P14[29],P3[15],P10[15],P8[16],P2[5],P5[238],P7[34],P0[332],P4[58]

,P12[132],P13[129],P1[79],P9[45],P11[39],P15[92],P6[297]

23 P10[19],P8[14],P5[223],P2[42],P14[59],P13[180],P4[55],P6[126]

,P15[66],P12[143],P7[161],P1[172],P9[97],P11[30],P0[86],P3[53]

24 P7[67],P12[83],P11[36],P3[60],P0[232],P2[13],P15[46],P9[54],P10[25]

,P4[27],P13[159],P5[286],P1[99],P14[63],P6[76],P8[48]

25 P14[20],P8[56],P5[196],P11[46],P6[38],P9[114],P12[144],P7[182]

,P15[42],P0[150],P2[15],P3[38],P4[11],P13[107],P10[8],P1[129]

26 P14[62],P6[419],P13[127],P1[28],P10[13],P4[46],P9[88],P3[68],P7[32]

,P8[65],P2[28],P5[187],P15[23],P12[80],P0[69],P11[20]

27 P4[83],P0[286],P9[59],P5[38],P6[191],P3[47],P13[92],P11[5],P14[56]

,P15[94],P7[62],P1[27],P12[123],P8[22],P2[27],P10[6]

28 P6[206],P2[12],P7[154],P15[14],P11[41],P13[193],P3[39],P14[6]

,P9[92],P10[35],P12[141],P0[185],P5[118],P1[17],P8[50],P4[1]

29 P13[13],P6[99],P9[18],P14[42],P12[6],P15[88],P10[20],P1[15],P11[23]

,P5[68],P0[241],P7[205],P4[50],P8[54],P2[36],P3[21]

30 P15[7],P13[45],P7[70],P5[282],P9[25],P10[34],P6[11],P3[48],P11[3]

,P2[34],P1[107],P14[39],P8[3],P4[21],P12[100],P0[276]

31 P15[69],P2[17],P5[233],P4[57],P7[175],P11[31],P14[25],P8[17],P3[4]

,P0[70],P12[9],P1[130],P13[43],P9[65],P10[42],P6[493]

The bits are selected by a 5 bit code taken from the data selector. This is formed from data selector bits:

29,31,8,19,61

The scrambler lfsr is initially loaded with a mixture of the 8 data bits, and

the 32 entrophy bits. There are 32 possible loadings. These are controlled by

5 bits from the data selector as follows:

10,0,51,42,28

The following tables are the 32 bits loaded into the scrambler before stepping.

They are selected by the 5 bits mentioned above:

sel bits

0 e[31],e[29],e[8],e[20],e[16],e[13],e[3],e[30],e[4],data[1],e[26],e[12],e[14]

,data[2],e[17],e[10],e[9],data[0],e[18],data[7],e[7],e[25],e[15],data[4]

,e[19],e[24],data[6],e[1],data[5],data[3],e[0],e[21]

1 data[2],e[15],e[20],data[1],e[14],e[21],data[0],e[7],e[0],e[12],e[25],data[3]

,e[1],e[13],data[4],data[6],e[19],e[11],e[10],data[5],data[7],e[8],e[23]

,e[30],e[28],e[17],e[29],e[2],e[16],e[5],e[4],e[31]

2 e[0],e[27],e[15],e[1],e[16],e[10],e[3],e[6],e[17],data[0],data[4],data[1]

,e[23],e[24],e[12],data[2],e[31],e[30],e[2],data[6],e[28],data[5],e[8]

,data[7],e[21],e[29],data[3],e[9],e[4],e[5],e[7],e[13]

3 e[20],e[28],e[31],data[6],data[0],e[15],data[3],e[1],e[0],e[16],data[5]

,e[10],e[3],e[4],e[5],e[22],data[4],e[17],e[19],e[26],e[2],data[7],data[1]

,e[12],e[7],e[18],e[24],data[2],e[29],e[11],e[14],e[23]

4 e[11],e[15],data[2],e[22],e[31],e[9],data[6],e[26],e[10],data[1],e[29],e[17]

,data[7],e[20],e[24],data[5],e[0],e[2],e[5],e[1],data[4],e[14],e[3],e[7]

,data[0],e[21],e[6],e[8],e[23],e[13],data[3],e[4]

5 data[7],e[14],e[3],data[5],e[17],data[0],e[13],data[1],e[12],e[29],e[20]

,e[18],e[5],e[11],e[30],e[9],e[26],e[24],e[21],e[8],e[15],e[7],e[25],data[3]

,e[19],e[31],e[0],data[6],e[6],data[2],data[4],e[23]

6 e[4],e[11],e[7],e[1],e[9],e[3],e[5],e[2],e[24],e[13],e[18],data[7],e[28]

,e[0],e[10],data[6],data[1],e[27],e[29],e[30],data[0],data[5],e[31],e[6]

,data[2],e[21],e[22],e[25],e[16],data[3],data[4],e[8]

7 e[12],e[1],e[11],data[3],e[15],e[18],e[2],data[4],e[20],data[1],data[5]

,e[0],data[2],e[19],e[31],data[0],e[7],e[16],data[7],e[9],e[29],e[22],e[23]

,e[6],data[6],e[25],e[21],e[13],e[5],e[14],e[3],e[27]

8 data[5],e[19],e[29],e[16],e[22],data[3],e[26],data[4],e[1],e[31],e[3],e[2]

,e[21],e[10],e[17],e[15],data[6],e[28],e[14],data[1],e[0],e[7],data[0]

,e[30],e[11],e[27],e[8],e[23],e[20],e[4],data[7],data[2]

9 e[0],e[5],e[26],e[1],data[0],data[2],e[22],e[31],e[6],e[27],data[3],e[18]

,e[21],e[8],e[2],e[14],e[23],e[19],e[28],e[13],e[11],data[1],data[4],data[7]

,e[24],data[6],e[29],e[16],e[17],e[25],e[4],data[5]

10 e[18],e[31],e[1],e[27],e[19],e[3],data[3],e[12],e[5],e[23],data[7],data[6]

,e[24],e[30],e[16],data[0],e[17],data[4],e[7],data[2],e[26],e[29],e[4]

,e[11],e[6],e[15],e[20],data[5],e[8],e[14],e[22],data[1]

11 data[0],e[15],e[18],e[14],e[7],data[7],data[3],data[2],e[16],e[13],e[4]

,e[28],e[19],e[5],e[8],data[5],data[4],data[1],e[3],data[6],e[24],e[17]

,e[21],e[22],e[6],e[27],e[11],e[23],e[26],e[29],e[2],e[20]

12 e[18],e[6],e[4],data[0],data[1],e[1],e[21],e[13],e[17],e[16],data[6],e[28]

,e[29],data[2],e[31],e[12],e[23],e[9],e[8],e[5],e[27],e[30],e[2],e[24]

,data[4],data[5],data[7],e[26],data[3],e[15],e[0],e[19]

13 e[20],e[2],e[16],e[6],e[10],e[22],data[3],e[3],data[4],e[30],e[4],e[1],e[5]

,e[11],data[5],e[19],e[7],e[31],e[27],data[7],e[21],e[25],e[28],data[1]

,e[26],e[13],data[0],data[6],data[2],e[12],e[0],e[18]

14 e[6],e[21],e[16],data[6],e[12],e[28],e[4],data[7],e[27],e[26],e[29],e[2]

,e[13],e[18],data[3],e[11],data[2],e[0],e[19],data[5],e[25],e[8],e[17]

,e[7],data[1],e[31],data[4],e[24],e[14],e[20],e[10],data[0]

15 data[5],e[29],e[16],e[18],e[2],data[0],e[24],e[26],e[23],data[4],data[6]

,e[11],data[3],data[1],e[19],e[0],e[14],e[15],e[12],e[25],data[2],data[7]

,e[6],e[3],e[9],e[27],e[28],e[20],e[8],e[31],e[1],e[30]

16 e[3],e[31],e[12],e[15],e[7],e[5],e[27],e[25],e[17],e[28],data[3],e[20],data[0]

,data[4],e[24],e[16],e[13],data[6],e[21],e[0],e[11],data[5],data[7],e[1]

,e[4],data[2],e[8],e[9],e[26],e[10],e[30],data[1]

17 e[25],e[4],data[4],e[14],e[0],e[18],data[7],e[7],data[0],e[1],data[3],data[2]

,data[1],data[5],e[5],e[22],e[16],e[12],e[24],e[17],e[13],e[29],e[9],e[11]

,e[20],e[30],e[3],data[6],e[28],e[8],e[23],e[26]

18 e[17],data[3],e[5],e[8],e[10],e[2],e[30],e[23],data[0],e[3],data[4],e[15]

,e[25],e[9],e[14],data[6],data[5],e[1],data[1],e[18],e[16],e[28],data[2]

,e[4],e[31],e[21],e[27],data[7],e[13],e[22],e[19],e[26]

19 e[29],data[6],data[4],e[9],e[28],e[4],e[17],data[5],e[5],e[26],e[25],e[8]

,data[0],e[3],e[10],e[12],e[6],e[27],data[3],e[22],e[31],e[0],data[7],data[1]

,e[21],e[20],e[16],data[2],e[13],e[11],e[30],e[18]

20 e[26],e[7],data[2],e[5],e[4],e[8],e[24],e[20],e[2],e[15],e[31],data[1],e[6]

,e[3],e[16],data[7],e[19],e[21],e[10],e[23],e[9],e[28],data[5],e[12],e[0]

,data[6],e[29],data[0],data[3],e[13],e[1],data[4]

21 e[10],e[20],e[24],data[0],e[4],e[21],e[8],e[17],e[30],e[6],e[5],data[6]

,e[31],e[3],data[7],e[0],data[4],e[27],e[2],e[13],data[3],e[23],data[2]

,e[26],e[9],e[25],data[5],e[29],e[1],data[1],e[12],e[11]

22 e[17],e[30],e[13],data[3],e[15],e[14],data[2],e[12],data[7],e[18],e[31]

,e[22],e[25],data[0],e[4],e[8],e[19],data[6],e[3],data[5],e[2],e[28],e[1]

,e[6],e[11],e[5],data[4],data[1],e[21],e[20],e[23],e[27]

23 e[24],data[7],e[17],data[4],e[22],e[19],data[6],e[30],e[14],e[28],e[23]

,data[1],data[5],e[7],e[18],e[11],e[5],e[27],e[26],e[2],e[9],e[25],e[29]

,e[16],e[13],e[6],e[3],data[3],data[2],data[0],e[20],e[12]

24 e[1],e[24],data[5],e[3],e[15],e[10],e[26],e[31],e[4],data[4],e[16],data[6]

,e[27],data[0],e[13],e[29],e[9],e[8],e[19],e[22],e[20],data[3],e[18],data[2]

,data[1],e[23],e[5],e[7],e[14],e[25],e[17],data[7]

25 e[30],e[17],data[4],data[3],e[20],e[1],e[31],data[0],e[27],e[23],e[13],e[2]

,data[5],e[24],e[25],e[6],e[19],data[2],e[22],e[3],e[12],data[6],e[29]

,e[9],e[10],e[5],data[1],e[11],data[7],e[14],e[28],e[18]

26 data[1],e[23],e[28],data[4],e[12],e[9],data[6],e[22],e[1],e[8],e[5],e[6]

,e[4],data[0],e[24],e[18],e[30],e[17],e[16],e[20],e[7],data[3],e[15],data[7]

,e[10],e[26],e[25],e[2],data[5],e[3],e[29],data[2]

27 e[3],e[23],e[17],data[5],e[30],e[29],e[7],e[2],e[24],e[18],e[28],e[11],e[20]

,e[12],data[1],e[5],e[22],e[25],data[0],e[21],e[13],data[4],e[8],data[6]

,e[15],data[7],e[16],data[3],e[26],e[10],e[14],data[2]

28 e[23],data[4],e[18],data[7],e[12],data[3],e[8],e[19],e[4],e[14],e[21],e[10]

,e[15],e[24],data[0],e[22],e[7],e[11],e[17],e[3],e[16],data[1],e[13],e[27]

,e[6],e[25],data[6],e[2],data[2],data[5],e[20],e[9]

29 e[23],e[19],e[2],e[0],e[18],e[5],e[1],e[22],e[25],data[0],data[3],e[29]

,e[15],e[11],e[7],data[5],e[9],e[28],e[17],data[7],data[2],data[4],e[12]

,e[16],e[24],e[21],e[8],e[31],data[1],e[26],data[6],e[4]

30 e[29],e[31],e[13],e[23],e[14],data[7],e[11],data[6],data[5],e[4],data[3]

,e[3],data[0],e[26],e[10],e[17],e[1],e[5],data[2],e[18],e[16],e[12],e[25]

,data[1],e[0],data[4],e[8],e[15],e[24],e[27],e[30],e[21]

31 e[9],e[2],e[28],e[16],e[29],data[4],data[0],e[21],e[20],data[1],data[3]

,e[24],e[12],e[18],e[13],e[6],data[6],e[8],data[5],e[30],e[19],e[22],e[26]

,e[0],data[2],data[7],e[31],e[4],e[15],e[7],e[3],e[27]

The design has an interface to load the lfsrs. This interface consists of a write signal, twelve address, and 32 data bits. This interface is used to provide the initial lfsr values:

Name bits Comment

clk 1 Rising edge clock

rst 1 Active high asynchronous reset

write 1 Write to an lfsr

addr 12 Address of lfsr register to write

lfsrdin 32 Data written to lfsr registers

The lfsrs are addressed according to the following address map. Note that unused bits are ignored on write.

addr LFSR

(hex)

01e dataselector[31:0]

01f dataselector[63:32]

020 Poly0[31:0]

021 Poly0[63:32]

022 Poly0[95:64]

023 Poly0[127:96]

024 Poly0[159:128]

025 Poly0[191:160]

026 Poly0[223:192]

027 Poly0[255:224]

028 Poly0[287:256]

029 Poly0[319:288]

02a Poly0[351:320]

02b Poly0[383:352]

02c Poly0[415:384]

02d Poly0[447:416]

02e Poly0[449:448]

033 Poly1[31:0]

034 Poly1[63:32]

035 Poly1[95:64]

036 Poly1[127:96]

037 Poly1[159:128]

038 Poly1[184:160]

03e Poly2[31:0]

03f Poly2[42:32]

046 Poly3[31:0]

047 Poly3[63:32]

048 Poly3[72:64]

04f Poly4[31:0]

050 Poly4[63:32]

051 Poly4[85:64]

054 Poly5[31:0]

055 Poly5[63:32]

056 Poly5[95:64]

057 Poly5[127:96]

058 Poly5[159:128]

059 Poly5[191:160]

05a Poly5[223:192]

05b Poly5[255:224]

05c Poly5[287:256]

05d Poly5[300:288]

065 Poly6[31:0]

066 Poly6[63:32]

067 Poly6[95:64]

068 Poly6[127:96]

069 Poly6[159:128]

06a Poly6[191:160]

06b Poly6[223:192]

06c Poly6[255:224]

06d Poly6[287:256]

06e Poly6[319:288]

06f Poly6[351:320]

070 Poly6[383:352]

071 Poly6[415:384]

072 Poly6[447:416]

073 Poly6[479:448]

074 Poly6[511:480]

075 Poly6[527:512]

07a Poly7[31:0]

07b Poly7[63:32]

07c Poly7[95:64]

07d Poly7[127:96]

07e Poly7[159:128]

07f Poly7[191:160]

080 Poly7[211:192]

084 Poly8[31:0]

085 Poly8[63:32]

086 Poly8[69:64]

089 Poly9[31:0]

08a Poly9[63:32]

08b Poly9[95:64]

08c Poly9[126:96]

08e Poly10[31:0]

08f Poly10[49:32]

096 Poly11[31:0]

097 Poly11[52:32]

09f Poly12[31:0]

0a0 Poly12[63:32]

0a1 Poly12[95:64]

0a2 Poly12[127:96]

0a3 Poly12[146:128]

0a7 Poly13[31:0]

0a8 Poly13[63:32]

0a9 Poly13[95:64]

0aa Poly13[127:96]

0ab Poly13[159:128]

0ac Poly13[191:160]

0ad Poly13[197:192]

0af Poly14[31:0]

0b0 Poly14[63:32]

0b2 Poly15[31:0]

0b3 Poly15[63:32]

0b4 Poly15[95:64]

0b5 Poly15[115:96]

The data input interface consists of the following signals:

name bits Comment

pushin 1 Push of the 8 data bits

datain 8 Data to be scrambled

entrophy 32 Entrophy data to aid scrambling

The output interface consists of the following signals:

name bits Comment

pushout 1 Data is pushed out of the design

dataout 32 Scrambled result data

Your module name must be se14 in file se14.v