ASSIGNMENT Part 1 , 2 and 3 Report

Amatul-CS13B032,Sphoorti-CS13B042,Sahiti-CS13B043

1

The Name of CIPHER:LEC(Little Encryption Code)
Encrypt for World Peace !!!

2

Number of rounds present in the cipher are "7".

3

Structure of cipher is similar to SPN.
Keylength=32
Blocklength=32
Assuming Kr is the round key used in the round
We divide the input into 8 blocks of 4 bits each,the following are done in 1 round of cipher
1.Substitution:
4x4 sbox is used here
The operations in substitution are:
a.Finding inverse in field(2^4)
If input is 0000 ,then ouput is 0,inverse of input infield(2^4) otherwise
The irreducible polynomial used here is $x^4 + x^3 + 1$.
But this may ensure fixed points i.e
s(0000)=0000
s(0001)=0001
b.Xoring with an appropriate 4 bit number
c=0011
Xoring with 0011 after obtaining inverse ensures no fixed points
Substitution layer is the confusion layer.
2.Permutation layer:
This has 2 operations:
a.Linear Transformation
For ensuring permutation we use MDS matrix as they ensure high branch number
MDS matrix choosen M is

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}$$

We divide the input say a1a2a3a4a5a6a7a8(where ai corresponds to 1 block of 4 bits) and apply the transformation

M*

$$\begin{pmatrix} a1 & a2 \\ a3 & a4 \\ a5 & a6 \\ a7 & a8 \end{pmatrix}$$

b.Shifting
Let the input be b1b2b3b4b5b6b7b8 after applying linear transformation to given input,then it would result in b5b6b7b8b1b2b3b4 after applying shifting
Permutation layer is the diffusion layer in the cipher
3.Xoring with round key
This ensures mixing between round input and round key

4

We need to ensure that the total bias of random variables or propogation ratios after Nr rounds should be less than brute force attack i.e no of input pairs required should be greater than 2^{32}.This is done Finding active sboxes in each round on an average by properties of diffusion,because of the MDS matrix(of branch number 5) used in the diffusion layer,the no of active S-boxes after a round would be 4 i.e, if 1 bit or component is changed ,in the output 4 components are changed giving rise to 4 active S-boxes.So ,let us take after every round we get 4 active S-boxes starting with 1 in the beginning,after completing 6 rounds(one round less than the total rounds) we get on an average 6(4)=24 active S-boxes so in total 8.Because of the non-linear and other properties present in S-box we get 1/4 as the maximum propagation ratio and also maximum bias .Therefore $(1/4)^2 4=1/2^{48}$ would be maximum propagation.This make it worse than brute force attack which is $1/2^{32}$,therefore 7 rounds are chosen .It can be similarly proved for maximum bias.

5

The options for S-boxes are 4x4,6x4,3x2,8x8.If chosen 6x4 or 3x2 ,the S-box will be a compression S-box.In case of compression the output for multiple inputs will be same ,this can increase th bias because we xor and also it can increase propagation ratio,may be that is the reason DES has chosen different S-boxes .So we have concluded to use 4x4 or 8x8 AES type of S-boxes. As field inverse satisfies properties of balancedness and SAC, and as mentioned the advantages of using inverse and xoring to remove fixed points.The possible sizes for this would be 4x4 and 8x8 and we choose 4x4 to make it less complex.

0000	0011
0001	0010
0010	1111
0011	1011
0100	0101
0101	1100
0110	0111
0111	1101
1000	0000
1001	1110
1010	1000
1011	1001
1100	0001
1101	1010
1110	0100
1111	0110

Figure 1: .

6

As all operations are performed in the field of 2^4
1.For finding inverse of a given x in the field,we used the property of multiplicative group.This field forms multiplicative group of order 15,by generating elements in multiplicative group,we calculated inverses of all elements other than 0
2.After applying inverse we xor with 0011.
The mapping after applying xor is found to be
Here we see that there are no fixed points.

7

a.From the obtained mappings we see that each of the four functions of sbox satisfy balanced property(equal no.of zeros and 1s)
The reason for this is:
There are 2 operations in substitution 1.Finding inverse in field(2^4) if it is not 0 ,otherwise 0
i.This ensures high non linearity
ii.Properties of balancedness is satisfied for inverse because it is a permutation and all 16

possible values are present which implies that each of the 4 functions is balanced
2.Xoring with an appropriate 4 bit number
c=0011
This ensures that it has no fixed points,and properties of balancedness still holds after applying xor because on applying xor with a particular number to all 16 permuations it would still result in all 16 possibilities.
b.SAC is satisfied in 1st step,this was verified by choosing all α with hamming distance 1 and finding if $f(x) \bigoplus f(x \bigoplus \alpha)$ is balanced.
Also SAC is not violated as xoring with a particular number and would not affect SAC property i.e $f(x) \bigoplus f(x \bigoplus \alpha)$ is same as $(f(x) \bigoplus c) \bigoplus (f(x \bigoplus \alpha) \bigoplus c)$,hence if the original one satisfies balanced property,then after xoring also it satisfies.
c.The affine functions are found using WH matrix and then non-linearity is calculated by finding minimum hamming distance of the function with affine functions.
For each of the four functions non linearity is calculated and found to be 4.This exhibits high non-linearity

8

The Linear approximation Table is displayed in Fig:2 below:

16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	
8	6	10	12	8	10	10	8	12	6	10	8	8	6	6	8
8	10	8	6	10	8	6	8	10	4	10	8	12	10	8	10
8	4	10	6	10	6	8	12	10	10	8	8	8	8	10	10
8	8	6	10	12	8	10	10	6	10	8	8	10	10	4	8
8	10	8	10	8	10	8	10	6	8	6	8	10	4	10	12
8	10	6	8	6	8	8	10	12	10	6	12	10	8	8	6
8	8	8	12	10	6	6	6	8	8	8	12	6	10	10	10
8	4	6	10	6	10	4	8	8	8	6	6	10	10	8	8
8	6	4	6	6	8	10	8	8	6	8	10	6	8	6	12
8	10	10	8	8	6	6	8	10	8	4	6	6	8	4	10
8	8	8	8	8	8	4	12	6	6	10	10	6	6	6	6
8	8	4	8	10	6	6	6	10	10	10	6	8	4	8	8
8	6	10	8	6	4	8	6	6	8	8	10	12	6	6	8
8	6	8	6	12	10	8	6	8	6	4	10	8	6	8	6
8	8	6	10	8	4	10	10	8	4	6	6	8	8	10	6

Figure 2: Linear approximation table.

9

The differential distribution table is displayed in Fig:4 below

10

The diffusion layer has 2 parts .Mix columns using linear transformation and then a permuation .
First part:

For Linear transformation ,MDS matrix over finite field (2^4) is used : A=

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}$$

This one can be checked that it is MDS matrix :All the submatrices are non-singular in field (2^4) .This can be checked by taking determinants of all submatrices.The necessary and sufficient condition for matrix to be MDS is:If A is a (m x n)matrix ,Make a matrix A'=($I_r \mid A$) where I_r is identity matrix n x n ,now if all the submatrix obtained by deleting m rows should be non-singular .This is verified for the given matrix and it satisfies.Actually this the MDS matrix used in AES for finite field(2^8) but because the numbers are all small the det values,multiplication are all same even in finite field(2^4).That is why the inverse is also same here.

The inverse is: A^{-1}=

$$\begin{pmatrix} E & B & D & 9 \\ 9 & E & B & D \\ D & 9 & E & B \\ B & D & 9 & E \end{pmatrix}$$

The inverse can be checked by following the traditional method of finding the det of matrix A and also adjoint of A.All calculations(multiplication,addition and reduction) done in the field.
This diffusion matrix has branch number 5 ,this helps is great diffusion creating lot of active S-boxes and thereby resulting in decrease in number of rounds,other wise because the S-boxes propagation are like 1/4 we have to take lot of rounds to achieve resistance against linear and differential cryptanalysis. if in put is :($(x_1,x_2,x_3,x_4,x_5,x_5,x_6,x_7,x_8)$
Output is : MIXColumns(x_1,x_3,x_5,x_7) =(x'_1,x'_3,x'_5,x'_7)
MIXColumns(x_2,x_4,x_6,x_8) =(x'_2,x'_4,x'_6,x'_8) Second Part:
The block is divided into 8 parts each with 4 bits:
if input for shifting is :($x_1,x_2,x_3,x_4,x_5,x_5,x_6,x_7,x_8$) The permutation is : ($x_2,x_4,x_6,x_8,x_1,x_3,x_5,x_7$)

11

The complete diffusion is achieved in 2 rounds here. Input:($x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8$) if input is changed in 1 bit let us suppose in some bit x_1 ,After S-box ,the 4 bits gets changed i.e, affecting 1 component of 8 and results is
($x'_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8$)
After Mix columns it will be diffused to 4 components
:($x'_1,x_2,x'_3,x_4,x'_5,x_6,x'_7,x_8$)
After shifting:($x_2,x_4,x_6,x_8,x'_1,x'_3,x'_5,x'_7$) Now second round: After S-boxes the state of changes is same,after Mix columns the change passes to all 8 components(because alternate

components are taken and mixed here): $(x_2'', x_4'', x_6'', x_8'', x_1'', x_3'', x_5'', x_7'')$
Thus the change propagated to all bits in 2 rounds.

12

The deadly trial for Linear attack is found to be :
Max_bias for deadly trial:-0.00000011920928955078
No of active S-boxes:22 overall
The bias for all these S-boxes for these inputs and outputs is 1/4. 0 0 13 0 0 0 0 0 –input to first round
0 0 5 0 0 0 0 0 –output of S-box
0 0 0 0 15 10 5 5 –output of Diffusion layer(input to second round)
0 0 0 0 9 10 15 15 –output of S-box
5 8 5 13 6 13 3 14 –output of Diffusion layer(input to third round)
15 1 15 12 8 5 7 10 –output of S-box
0 5 0 7 0 14 0 1 –output of Diffusion layer(input to fourth round)
0 15 0 3 0 10 0 8 –output of S-box
0 6 0 8 0 0 0 0 –output of Diffusion layer(input to fifth round)
0 8 0 1 0 0 0 0 –output of S-box
10 10 9 0 0 0 0 0 –output of Diffusion layer(input to sixth round)
10 10 2 0 0 0 0 0 –output of S-box
13 10 10 7 11 14 8 5–output of Diffusion layer(input to seventh round)

Here,the input and output means the a's and b's .

For the attack,we have to come from end and decrypt for seventh round and use the coefficients obtained from seventh round and calculate and bias and compare. The number of pairs required is approximately $0.00000011920928955078^{-2} = (11.9 * (10^{-8}))^(- 2) = 70.6 * 10^{12}$,this is far greater then $2^{32} = 4.29 * 10^9$

The Linear trial is neatly shown in Fig:5:

13

The deadly trial for Differential attack is found to be :
Max_bias for deadly trial:0.000000000000001776
No of active S-boxes:21 overall
The bias for all these S-boxes for these inputs and outputs is 1/4. 0 0 0 0 0 0 11 0 –input to first round
0 0 0 0 0 0 10 0–output of S-box
0 0 0 0 10 10 7 13–output of Diffusion layer(input to second round)
0 0 0 0 11 11 14 9 –output of S-box
2 13 13 0 5 10 4 14 –output of Diffusion layer(input to third round)
1 3 3 0 2 11 1 7–output of S-box
10 0 5 0 4 0 5 0–output of Diffusion layer(input to fourth round)

1 0 2 0 6 0 15 0 –output of S-box
0 0 0 0 13 0 7 0–output of Diffusion layer(input to fifth round)
0 0 0 0 9 0 14 0–output of S-box
0 0 0 0 7 12 0 12 –output of Diffusion layer(input to sixth round)
0 0 0 0 14 2 0 2–output of S-box
0 4 2 6 14 11 5 14–output of Diffusion layer(input to seventh round)

Here,the input and output means the a's and b's .

For the attack,we have to come from end and decrypt for seventh round and use the coefficients obtained from seventh round and calculate and bias and compare. The number of pairs required is approximately $0.0000000000000001776^{-1} = (17.8*(10^{-15}))^(-1) = 5.6 * 10^{13}$,this is far greater then $2^{32} = 4.29 * 10^9$

The Differential trial is neatly shown in Fig:6:

14

Modification for second question:The number of rounds is changed from 6 to 7.For linear and differential analysis ,we consider one round less (because for the last round we come from end.) and we analysed for 6 rounds ,so the number of rounds is actually 6+1=7.
Extension of answer for fourth question: The number of rounds required is conformed to be 7.For differential trail,The average maximum propagation was found to be $\epsilon = 1/2^{48}$,so the number of pairs required would be approximately c*(ϵ^{-1}) for "small" constant c.Here $\epsilon^{-1} = 2^{48}$ which is far greater than brute force complexity 2^{32} ,even the deadly trial is far greater than this as seen in previous question.So resistance to differential attack.
For Linear attack,the average number of active S-boxes for 6 rounds is 24 ,so the average maximum bias is $(2^2 3) * (1/4^{24})$ using piling up lemma $2^{k-1} * \prod_{i=1}^{k} \epsilon_{k-1}$ which is equal to $1/2^{25}$.Using this,the average number of pairs required is $c * \epsilon_{-2}$=$c * 2^{50}$ which is also far greater than 2^{32},even the deadly trial is far greater than 2^{32} as seen from previous question.Therefore ,it is resistant to Linear attack.Therefore the Cipher is proved to be resistant to both Linear and differential attack with number of rounds 7.

15

Our implementation is efficient in terms of number of operations.We did so by using lookup tables for mix columns.As our MDS matrix is

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}$$

we used 4 lookup tables each containing
T0=2x,x,x,3x
T1=3x,2x,x,x

T2=x,3x,2x,1x
T3=x,x,3x,2x
for each of the possible 16 values of x.(because 32 bit block is divided into 8 4 bit blocks(4 by 2 matrix) in our implementation for mix columns).Size of each look up table is 16*16 bytes(i.e 4 values are stored for each of the inputs=4*4 and no.of entries is 16),So size of 4 tables put together is 256*4 bytes=1024 bytes.Using these lookup tables there will be 8 substitution operations,8 permutations and 8 xoring operations,a total of 24 operations for each round.

16

No need to make any changes in previous questions.

17

The time taken for encryption for different file sizes is plotted.It is approximately linear with the file size as shown in Figure 3.

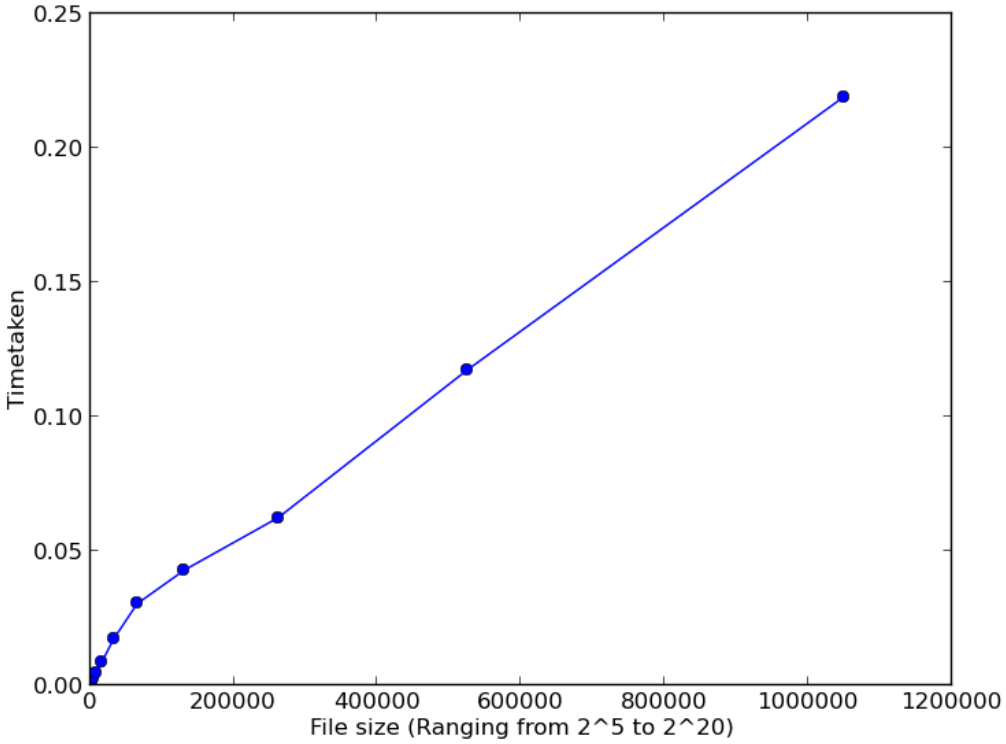

Figure 3: Filesize Vs time for encryption

18

All The required files are present in the folder.

16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	4	2	0	2	0	0	0	0	2	2	2	0	0	2	0
0	2	2	0	0	2	0	2	2	2	0	0	4	0	0	0
0	0	0	0	0	0	2	2	4	2	0	2	0	2	2	0
0	2	0	0	2	0	4	0	2	0	0	0	2	0	2	2
0	0	2	0	0	0	0	2	0	0	2	0	2	2	2	4
0	0	0	2	4	0	0	2	2	2	2	0	0	0	0	2
0	0	2	2	0	2	2	0	2	0	2	0	0	0	4	0
0	0	2	4	2	0	2	2	0	0	0	2	2	0	0	0
0	2	2	2	0	0	2	0	0	2	0	0	0	4	0	2
0	2	0	0	0	2	2	2	0	0	2	4	0	0	0	2
0	2	0	2	0	0	0	0	2	0	4	2	2	2	0	0
0	0	4	0	2	2	0	0	2	0	0	2	0	2	0	2
0	0	0	2	0	2	0	0	0	4	0	2	2	0	2	2
0	2	0	2	2	2	0	4	0	0	0	0	0	2	2	0
0	0	0	0	2	4	2	0	0	2	2	0	2	2	0	0

Figure 4: Differential distribution table.

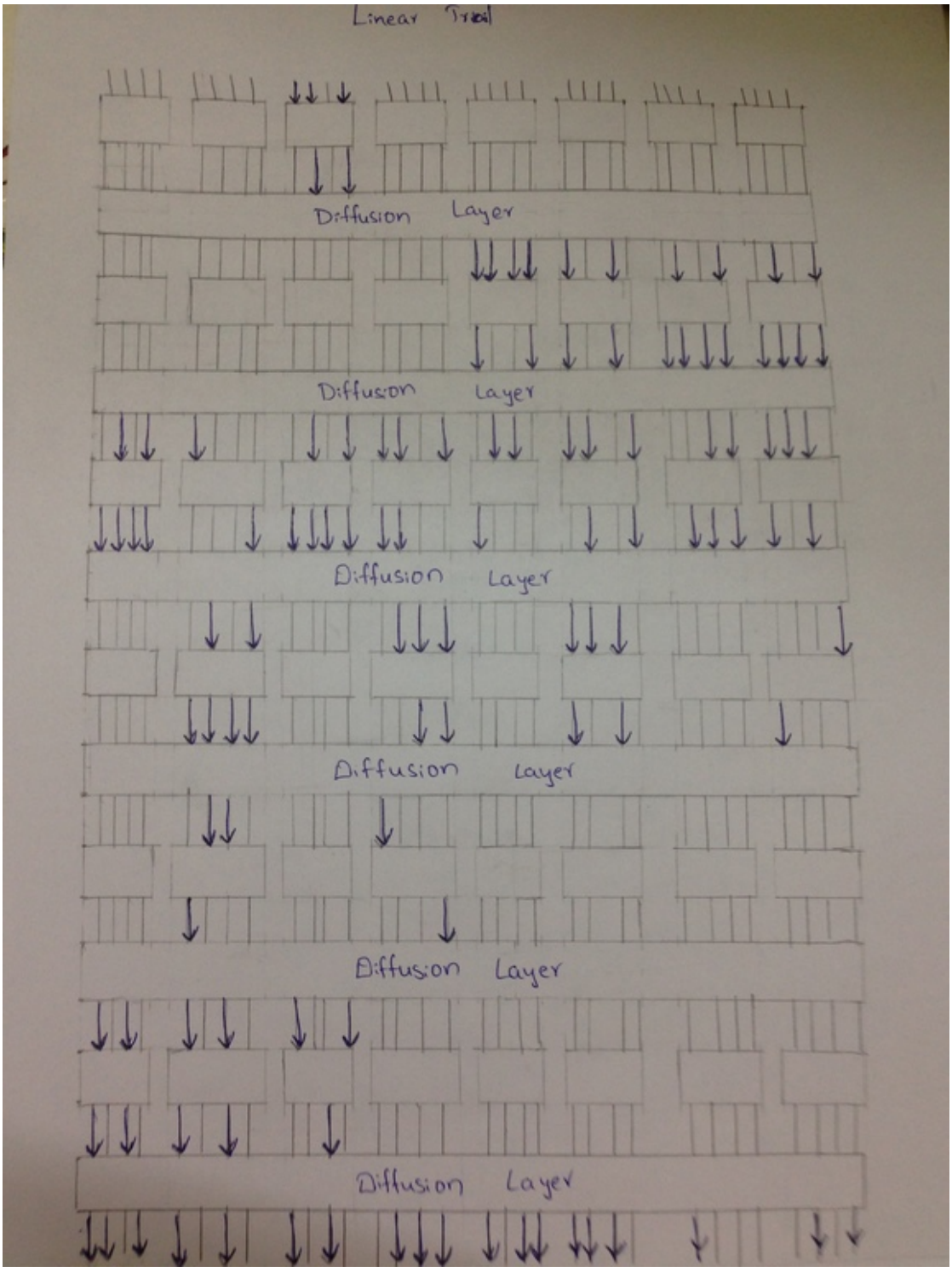

Figure 5: Linear trail

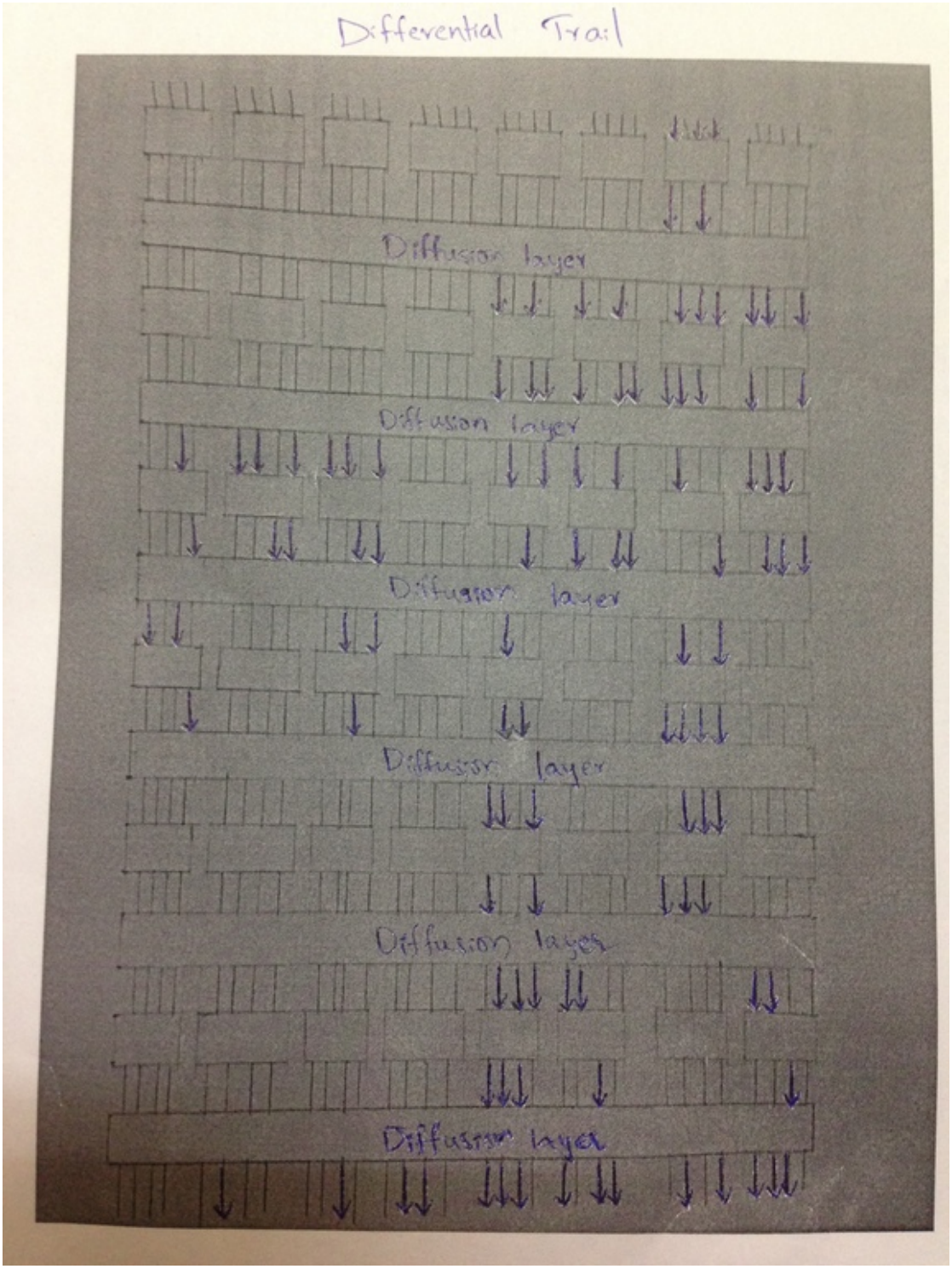

Figure 6: Differential trail