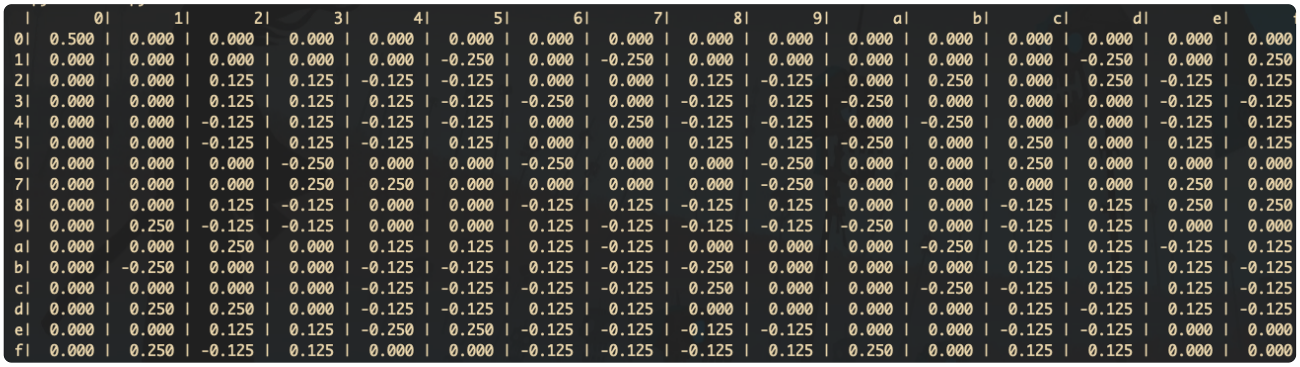
Linear Cryptanalysis

A block cipher based on substitution permutation network structure has in one round:

1. Sub-key mixing
2. S-box
3. Permutation (wire crossing)

After the last round there is an extra key mixing, otherwise it would be very easy to revert the last round.

To attack the PRESENT cipher, one comes up with the S-box linear approximation table. Then using this table one creates an (N-1) round approximation to attack a N round cipher.

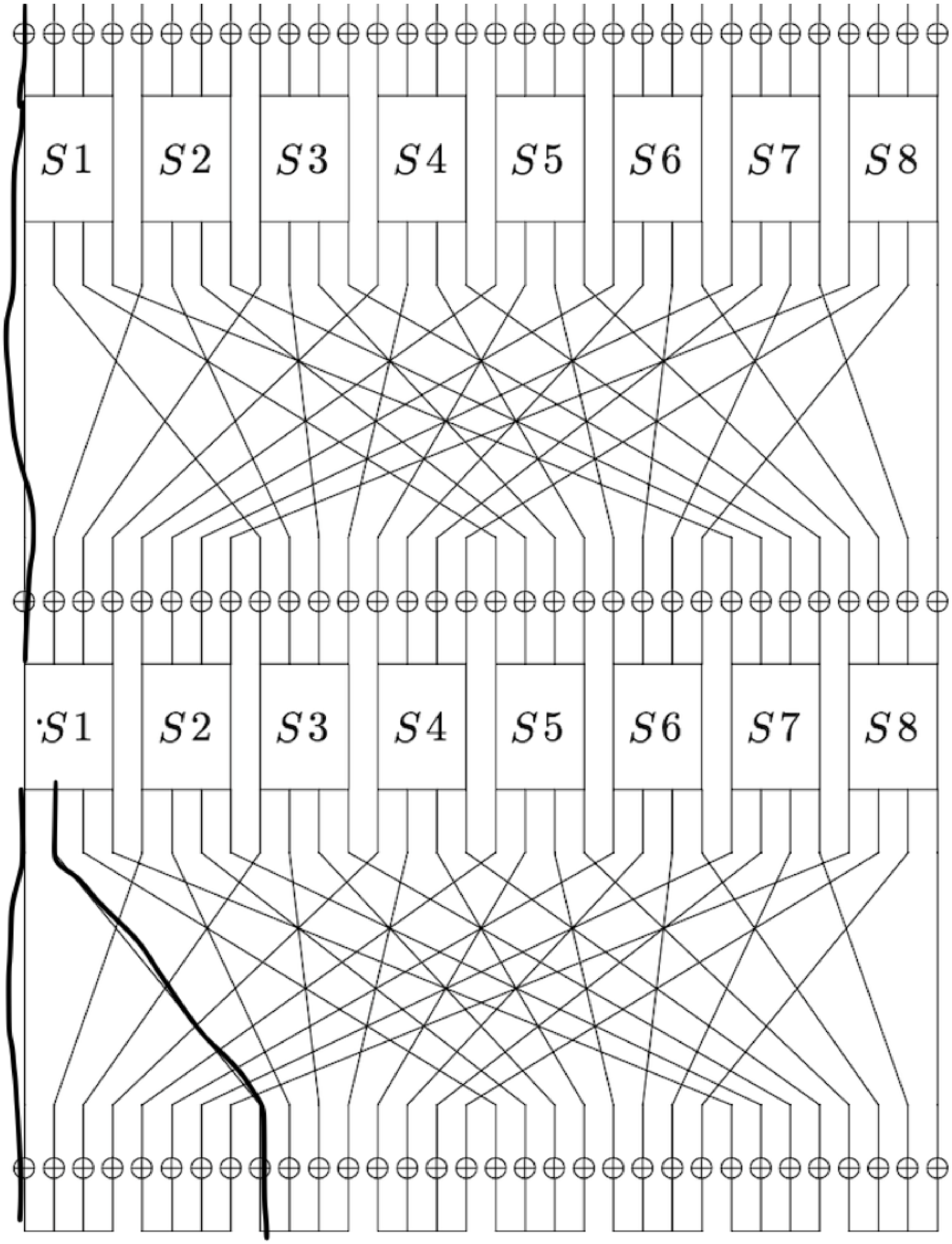


```
 |      0|      1|      2|      3|      4|      5|      6|      7|      8|      9|      a|      b|      c|      d|      e|
0|  0.500 |  0.000 |  0.000 |  0.000 |  0.000 |  0.000 |  0.000 |  0.000 |  0.000 |  0.000 |  0.000 |  0.000 |  0.000 |  0.000 |  0.000 |  0.000
1|  0.000 |  0.000 |  0.000 |  0.000 |  0.000 | -0.250 |  0.000 | -0.250 |  0.000 |  0.000 |  0.000 |  0.000 |  0.000 | -0.250 |  0.000 |  0.250
2|  0.000 |  0.000 |  0.125 |  0.125 | -0.125 | -0.125 |  0.000 |  0.000 |  0.125 | -0.125 |  0.000 |  0.250 |  0.000 |  0.250 | -0.125 |  0.125
3|  0.000 |  0.000 |  0.125 |  0.125 |  0.125 | -0.125 | -0.250 |  0.000 | -0.125 |  0.125 | -0.250 |  0.000 |  0.000 |  0.000 | -0.125 | -0.125
4|  0.000 |  0.000 | -0.125 |  0.125 | -0.125 | -0.125 |  0.000 |  0.250 | -0.125 | -0.125 |  0.000 | -0.250 |  0.000 |  0.000 | -0.125 |  0.125
5|  0.000 |  0.000 | -0.125 |  0.125 | -0.125 |  0.125 |  0.000 |  0.000 |  0.125 |  0.125 | -0.250 |  0.000 |  0.250 |  0.000 |  0.125 |  0.125
6|  0.000 |  0.000 |  0.000 | -0.250 |  0.000 |  0.000 | -0.250 |  0.000 |  0.000 | -0.250 |  0.000 |  0.000 |  0.250 |  0.000 |  0.000 |  0.000
7|  0.000 |  0.000 |  0.000 |  0.250 |  0.250 |  0.000 |  0.000 |  0.000 |  0.000 | -0.250 |  0.000 |  0.000 |  0.000 |  0.000 |  0.250 |  0.000
8|  0.000 |  0.000 |  0.125 | -0.125 |  0.000 |  0.000 | -0.125 |  0.125 | -0.125 |  0.125 |  0.000 |  0.000 | -0.125 |  0.125 |  0.250 |  0.250
9|  0.000 |  0.250 | -0.125 | -0.125 |  0.000 |  0.000 |  0.125 | -0.125 | -0.125 | -0.125 | -0.250 |  0.000 | -0.125 |  0.125 |  0.000 |  0.000
a|  0.000 |  0.000 |  0.250 |  0.000 |  0.125 |  0.125 |  0.125 | -0.125 |  0.000 |  0.000 |  0.000 | -0.250 |  0.125 |  0.125 | -0.125 |  0.125
b|  0.000 | -0.250 |  0.000 |  0.000 | -0.125 | -0.125 |  0.125 | -0.125 | -0.250 |  0.000 |  0.000 |  0.000 |  0.125 |  0.125 |  0.125 | -0.125
c|  0.000 |  0.000 |  0.000 |  0.000 | -0.125 | -0.125 | -0.125 | -0.125 |  0.250 |  0.000 |  0.000 | -0.250 | -0.125 |  0.125 |  0.125 | -0.125
d|  0.000 |  0.250 |  0.250 |  0.000 | -0.125 | -0.125 |  0.125 |  0.125 |  0.000 |  0.000 |  0.000 |  0.000 |  0.125 | -0.125 |  0.125 | -0.125
e|  0.000 |  0.000 |  0.125 |  0.125 | -0.250 |  0.250 | -0.125 | -0.125 | -0.125 | -0.125 |  0.000 |  0.000 | -0.125 | -0.125 |  0.000 |  0.000
f|  0.000 |  0.250 | -0.125 |  0.125 |  0.000 |  0.000 | -0.125 | -0.125 | -0.125 |  0.125 |  0.250 |  0.000 |  0.125 |  0.125 |  0.000 |  0.000
```

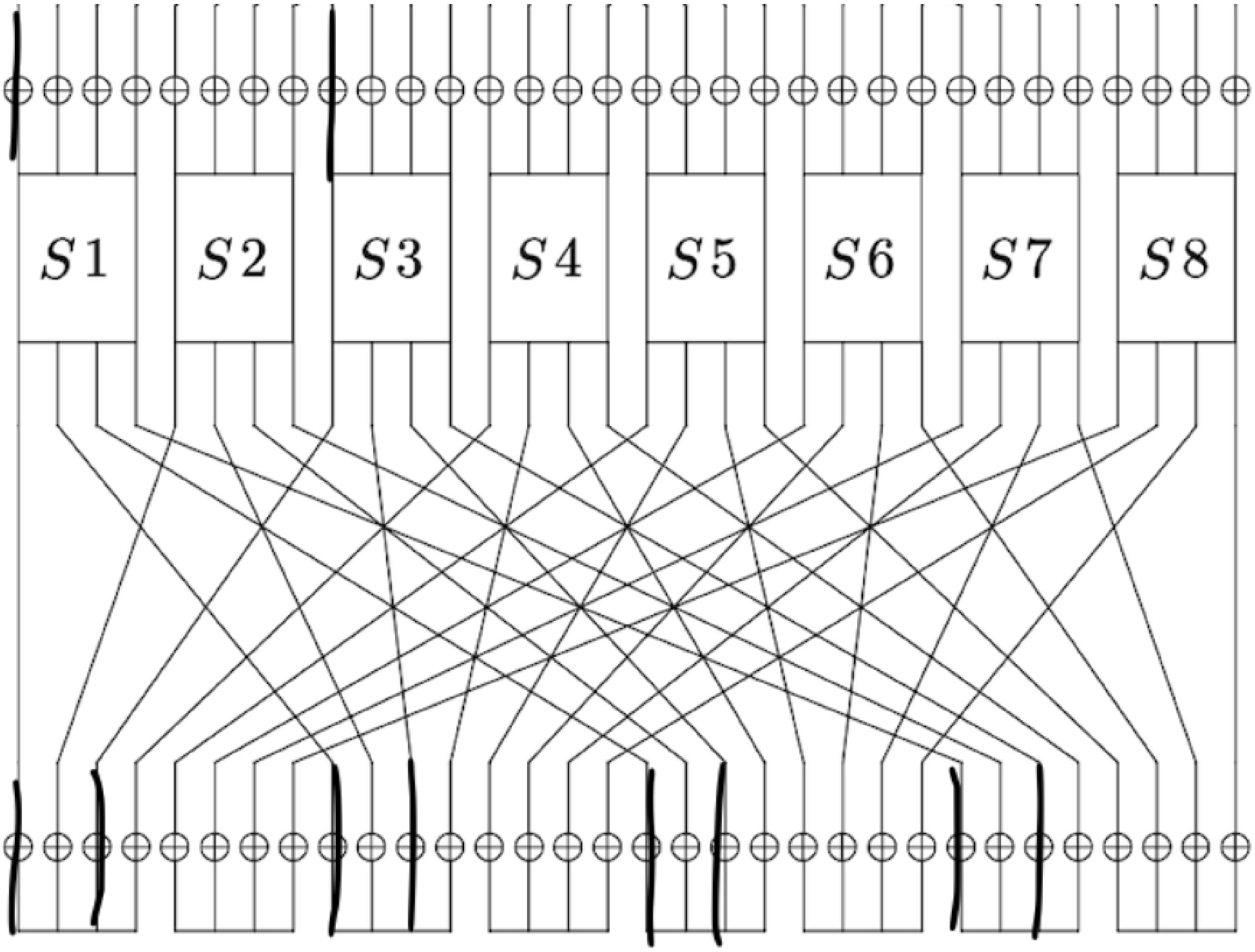
$a_1x_1, a_2x_2, a_3x_3, a_4x_4 => a_1a_2a_3a_4$

Then, data is generated or intercepted as {plaintext, ciphertext} pairs.

In the approximation, active S-boxes on layer N-1 are identified.



And corresponding keys are followed to the Nth layer (If permutation is done before the last key mixing). Then the target key mask is generated.



Using the target key mask, a key hypothesis is made and the ciphertexts are decrypted 1 round (this could be made with a previously implemented decrypt function taking (ciphertext, key, number_of_rounds) as parameters). Then applying the key again gives the cts corresponding to the N-1 th round

These decrypted ciphertexts are accumulated in a list, in a way they represent the output of encrypt(pts, k, N-1). Then the experimental bias is computed with the accumulated ciphertexts and corresponding plaintexts.

Then the key is selected corresponding to the highest bias.