Lecture Misc:
Read KeySchedule
Read Decryption in AES

plus Write a program on finding the inverse of a Galois field and then try to find if there is any relation between them.

Check how 1 bit flip can cause 4 bits flip on an average and if there is any relation between them.

What is non linearity in AES and other ciphers and how does it helps against attacks ?

1. **Key Whitening :** XOR with Sub Key at both input and output is sometimes referred to as Key Whitening.
2. Total subkeys required for AES is number of rounds + 1, so **question** can be why **Round + 1,** reason for this is first round takes k0 for input and k1 for output and similarly second round will take k1 as input and k2 as output. as shown in table below too. so 0th sub key is extra sub key.
    1. 1 => 0,1
    2. 2 => 1,2
    3. 3 => 2,3
    4. 4 => 3,4

Key Schedule :
K0 key on AES key Schedule is same as the original key and it is divided into 4 parts of 32 bit each. W[0], W[1], ..., W[43] are the total 32 bits parts of 128 bit key with 11 rounds of Key Schedule.

Different Key sizes have different key schedule but it is very similar for all 3 or them. Key schedule for 128 bit AES is shown below.

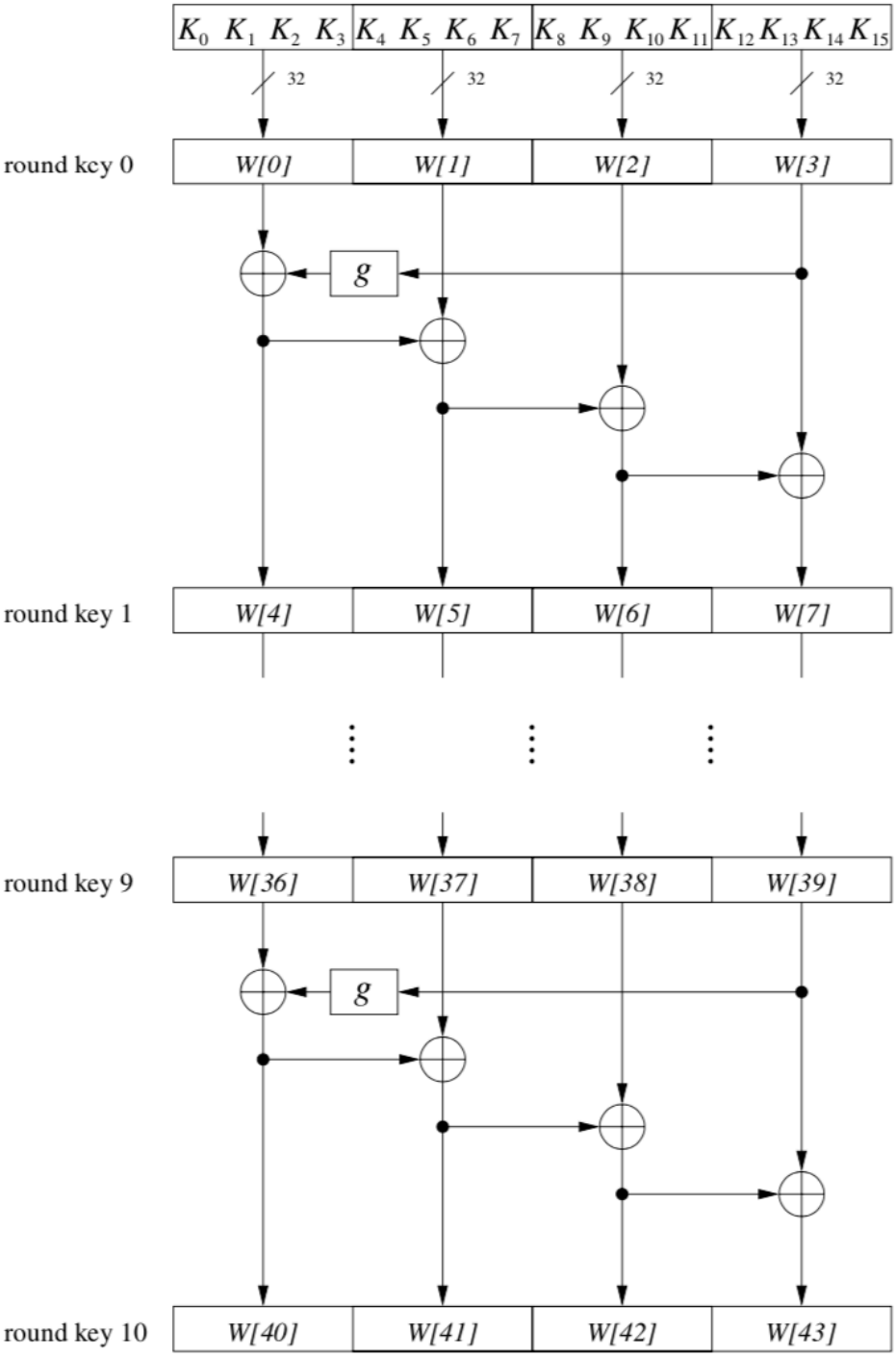

Fig. 4.5 AES key schedule for 128-bit key size

More on Key Schedule Internals :