Key Schedule

- Subkeys are derived recursively from the original 128/192/256-bit input key

- Each round has 1 subkey, plus 1 subkey at the beginning of AES

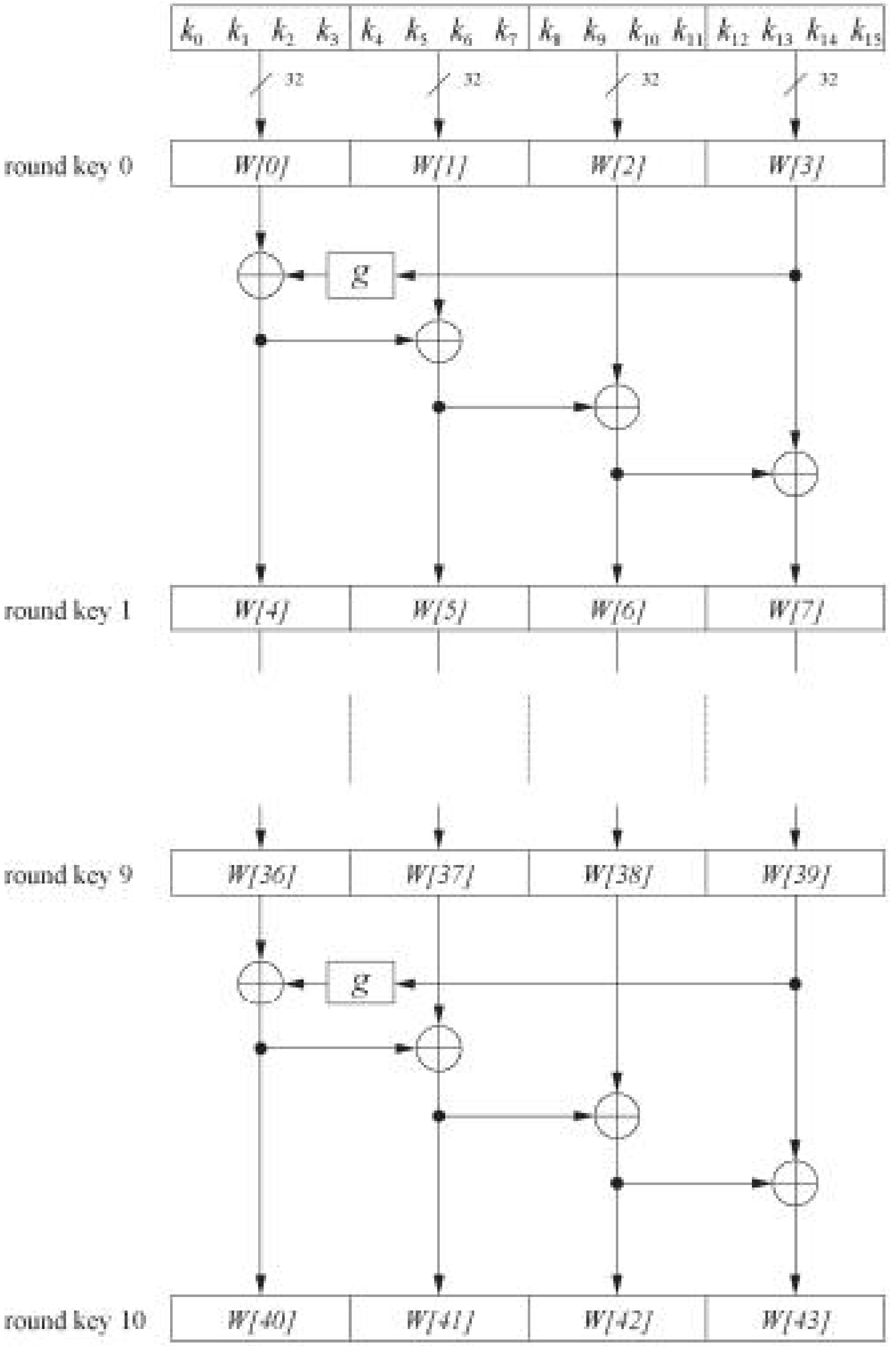
Key length (bits)	Number of subkeys
128	11
192	13
256	15

- Key whitening: Subkey is used both at the input and output of AES
  ⇒ # subkeys = # rounds + 1

- There are different key schedules for the different key sizes

Key Schedule

Example: Key schedule for 128-bit key AES



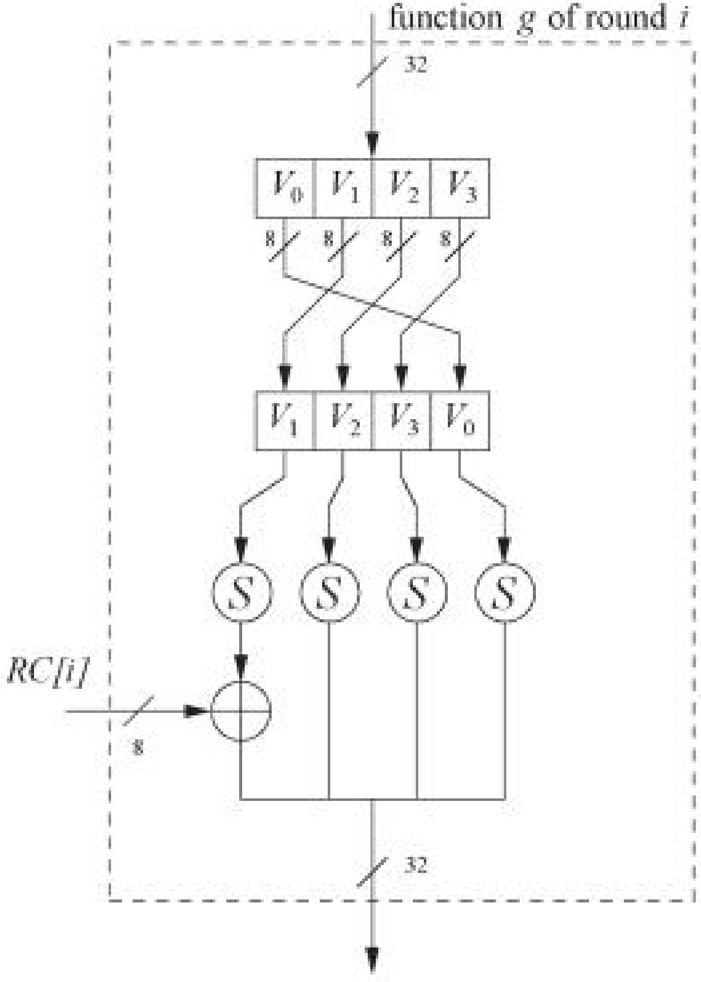
- Word-oriented: 1 word = 32 bits
- 11 subkeys are stored in *W[0]…W[3]*, *W[4]…W[7]*, … , *W[40]…W[43]*
- First subkey *W[0]…W[3]* is the original AES key

Key Schedule

- Function *g* rotates its four input bytes and performs a bytewise S-Box substitution
  ⇒ nonlinearity

- The round coefficient *RC* is only added to the leftmost byte and varies from round to round:

$$RC[1] = x^0 = (00000001)_2$$
$$RC[2] = x^1 = (00000010)_2$$
$$RC[3] = x^2 = (00000100)_2$$
$$\ldots$$
$$RC[10] = x^9 = (00110110)_2$$



- x^i represents an element in a Galois field
  (again, cf. Chapter 4.3 of *Understanding Cryptography*)