Advanced Encryption Standard (AES)

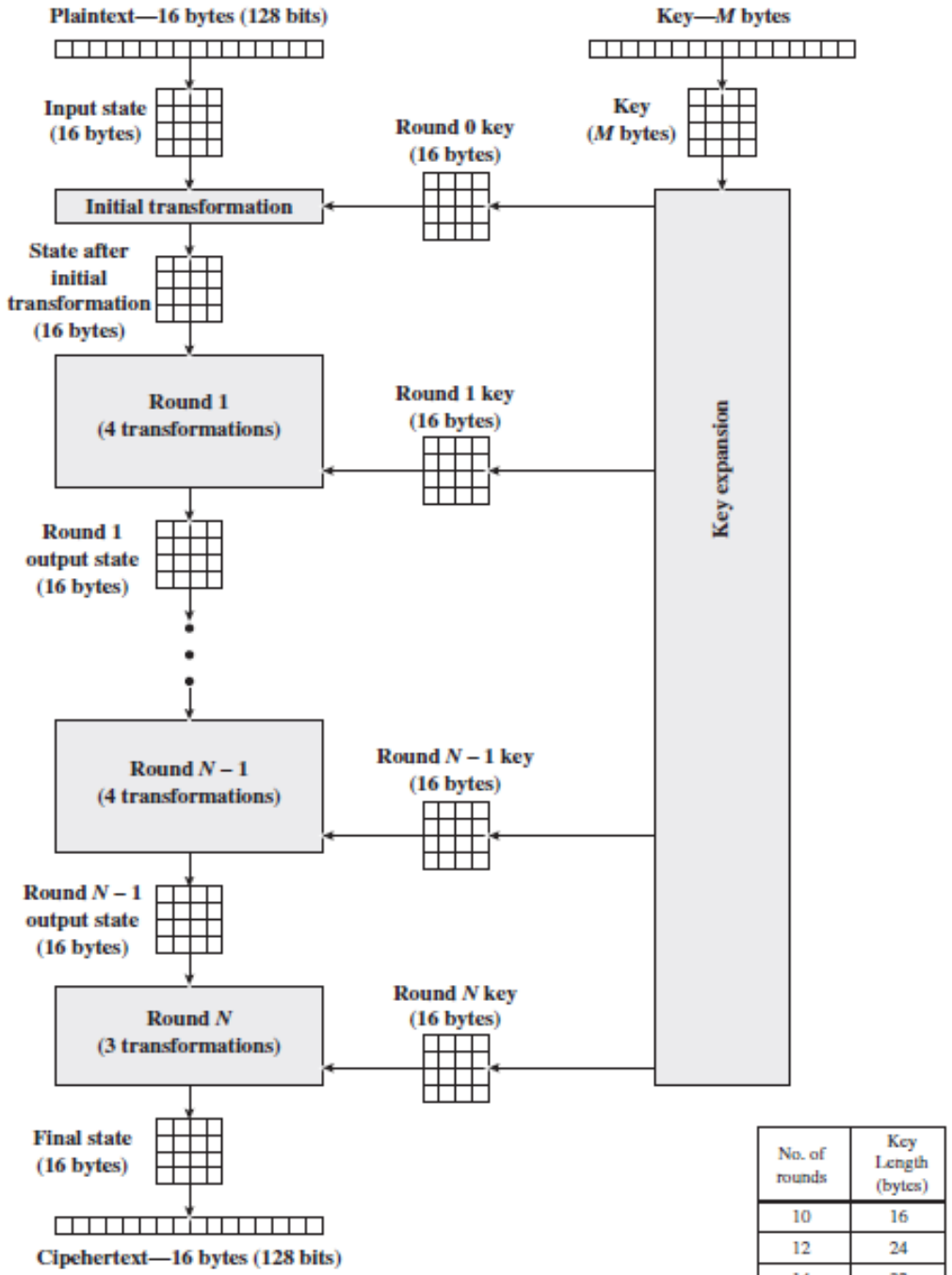
Dr. Shubhangi Sapkal

AES Structure

- The cipher takes a plaintext block size of 128 bits, or 16 bytes. The key length can be 16, 24, or 32 bytes (128, 192, or 256 bits).
- The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length.
- The input to the encryption and decryption algorithms is a single 128-bit block. This block is depicted as a 4 * 4 square matrix of bytes.
- Similarly, the key is depicted as a square matrix of bytes. This key is then expanded into an array of key schedule words.

AES Structure

- The cipher consists of N rounds, where the number of rounds depends on the key length: 10 rounds for a 16-byte key, 12 rounds for a 24-byte key, and 14 rounds for a 32-byte key.
- The first N - 1 rounds consist of four distinct transformation functions: SubBytes, ShiftRows, MixColumns, and AddRoundKey.
- The final round contains only three transformations, and there is a initial single transformation (AddRoundKey) before the first round, which can be considered Round 0.
- Each transformation takes one or more 4 * 4 matrices as input and produces a 4 * 4 matrix as output.
- Also, the key expansion function generates N + 1 round keys, each of which is a distinct 4 * 4 matrix. Each round key serves as one of the inputs to the AddRoundKey transformation in each round.



No. of rounds	Key Length (bytes)
10	16
12	24
14	32

Figure 1: AES Encryption structure

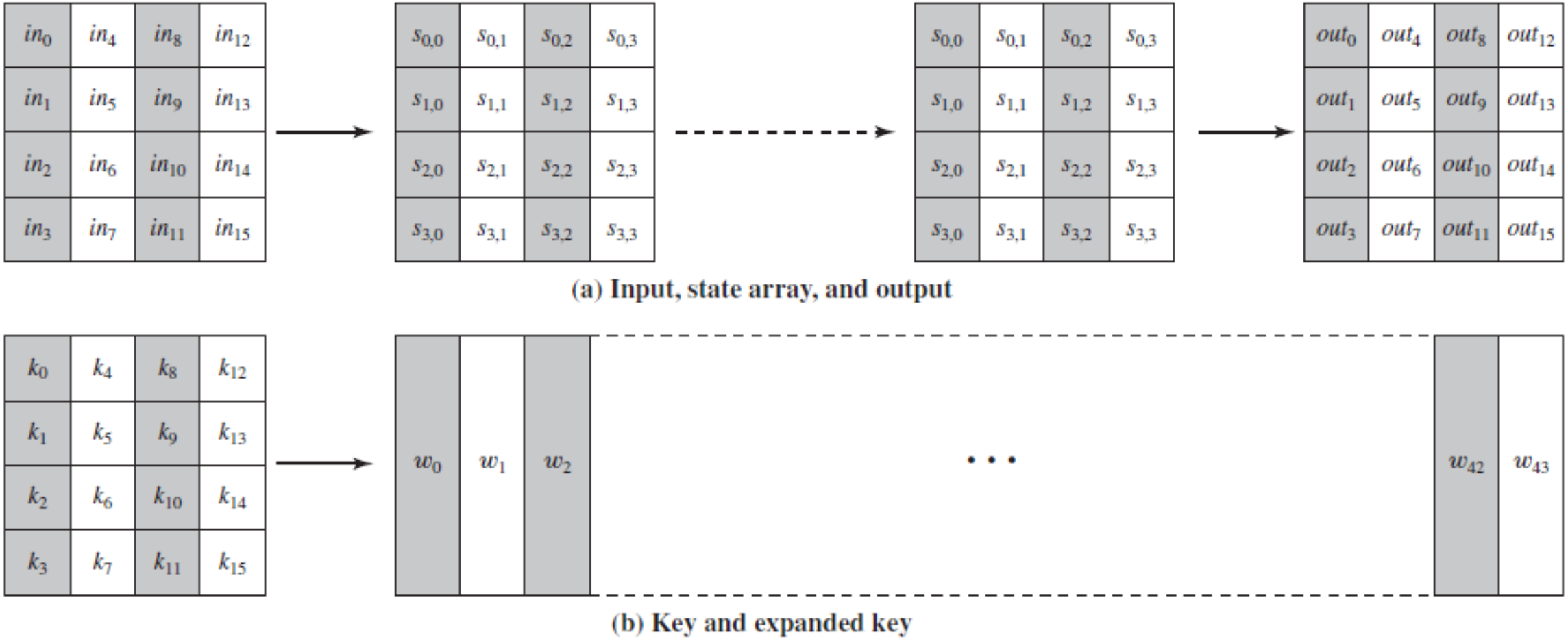


Figure 2: AES Key expansion

Table 1: AES Parameters

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size (words/bytes)	44/176	52/208	60/240

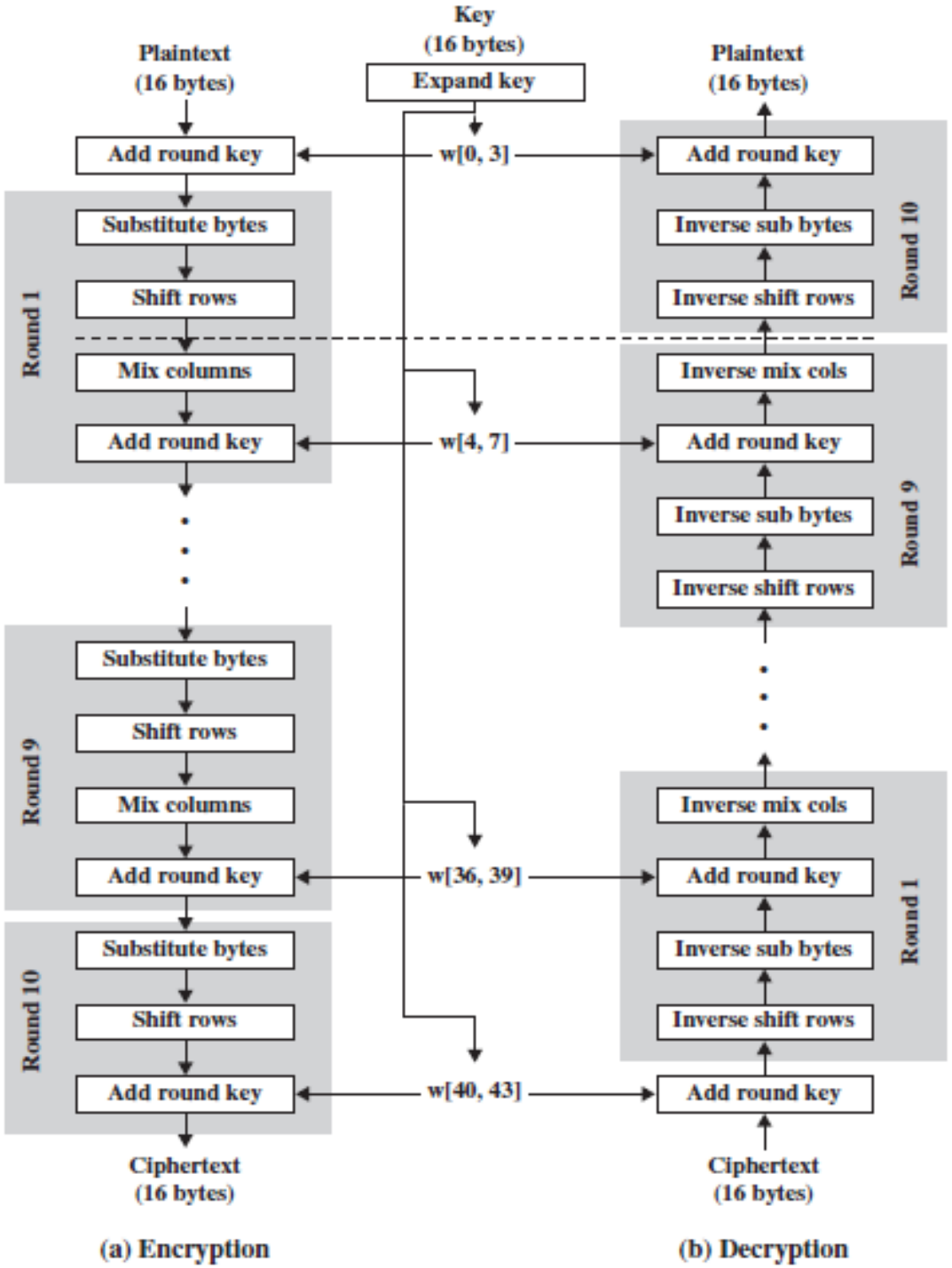


Figure 3: AES Encryption and Decryption

Figure 3 shows the AES cipher in more detail, indicating the sequence of transformations in each round and showing the corresponding decryption function.

AES Structure

- One noteworthy feature of this structure is that it is not a Feistel structure. In the classic Feistel structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. AES instead processes the entire data block as a single matrix during each round using substitutions and permutation.
- The key that is provided as input is expanded into an array of forty-four 32-bit words, **w**[*i*].
- Four different stages are used, one of permutation and three of substitution:
  - **Substitute bytes:** Uses an S-box to perform a byte-by-byte substitution of the block
  - **ShiftRows:** A simple permutation
  - **MixColumns:** A substitution that makes use of arithmetic over GF(2^8)
  - **AddRoundKey:** A simple bitwise XOR of the current block with a portion of the expanded key

AES Structure

- The structure is quite simple. For both encryption and decryption, the

cipher begins with an AddRoundKey stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages.

- Only the AddRoundKey stage makes use of the key. For this reason, the cipher begins and ends with an AddRoundKey stage. Any other stage, applied at the beginning or end, is reversible without knowledge of the key and so would add no security.

AES Structure

- Each stage is easily reversible. For the Substitute Byte, ShiftRows, and MixColumns stages, an inverse function is used in the decryption algorithm.
- For the AddRoundKey stage, the inverse is achieved by XORing the same round key to the block, using the result that A B B = A.
- The decryption algorithm makes use of the expanded key in reverse order. However, the decryption algorithm is not identical to the encryption algorithm.
- Once it is established that all four stages are reversible, it is easy to verify that decryption does recover the plaintext. In encryption and decryption, at each horizontal point, **State** is the same for both encryption and decryption.
- The final round of both encryption and decryption consists of only three stages.

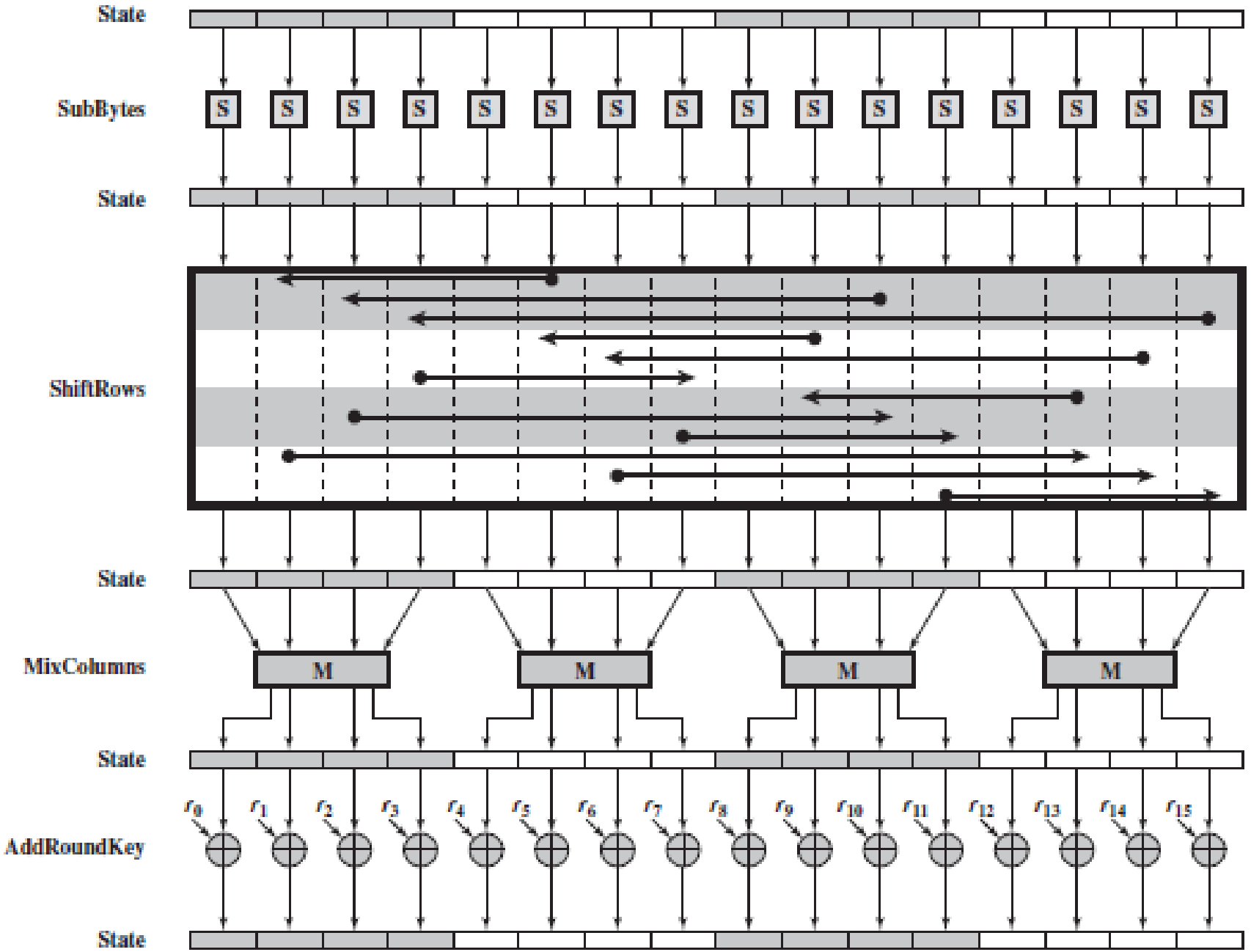


Figure 4: AES Encryption round