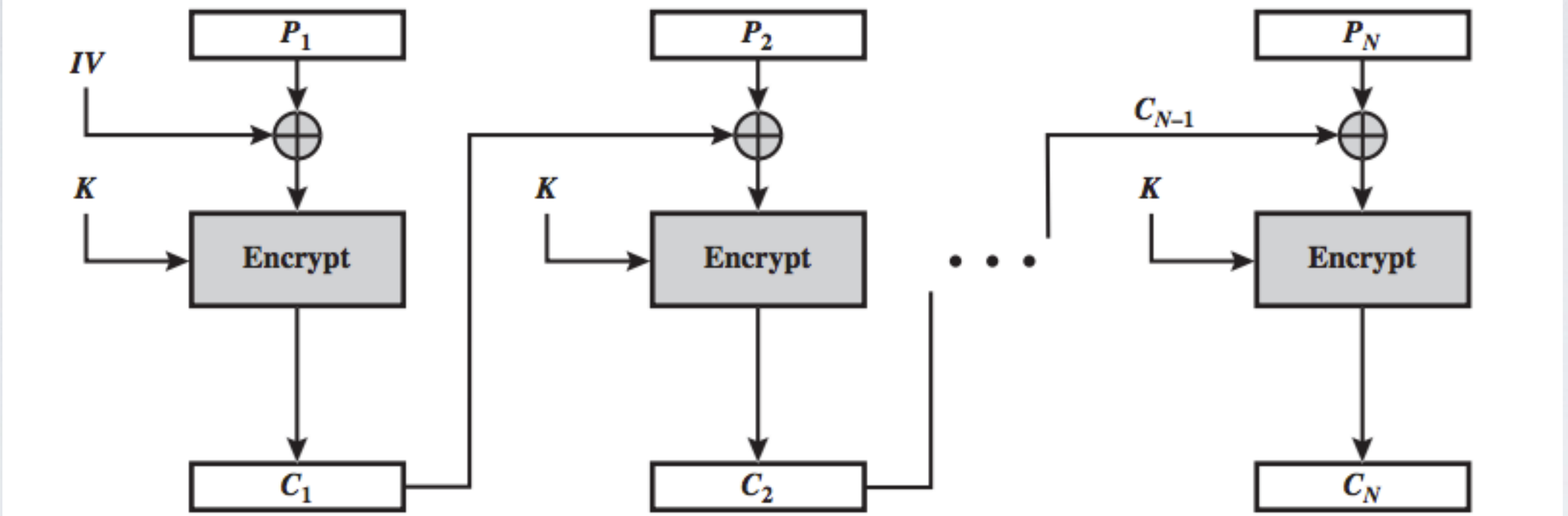
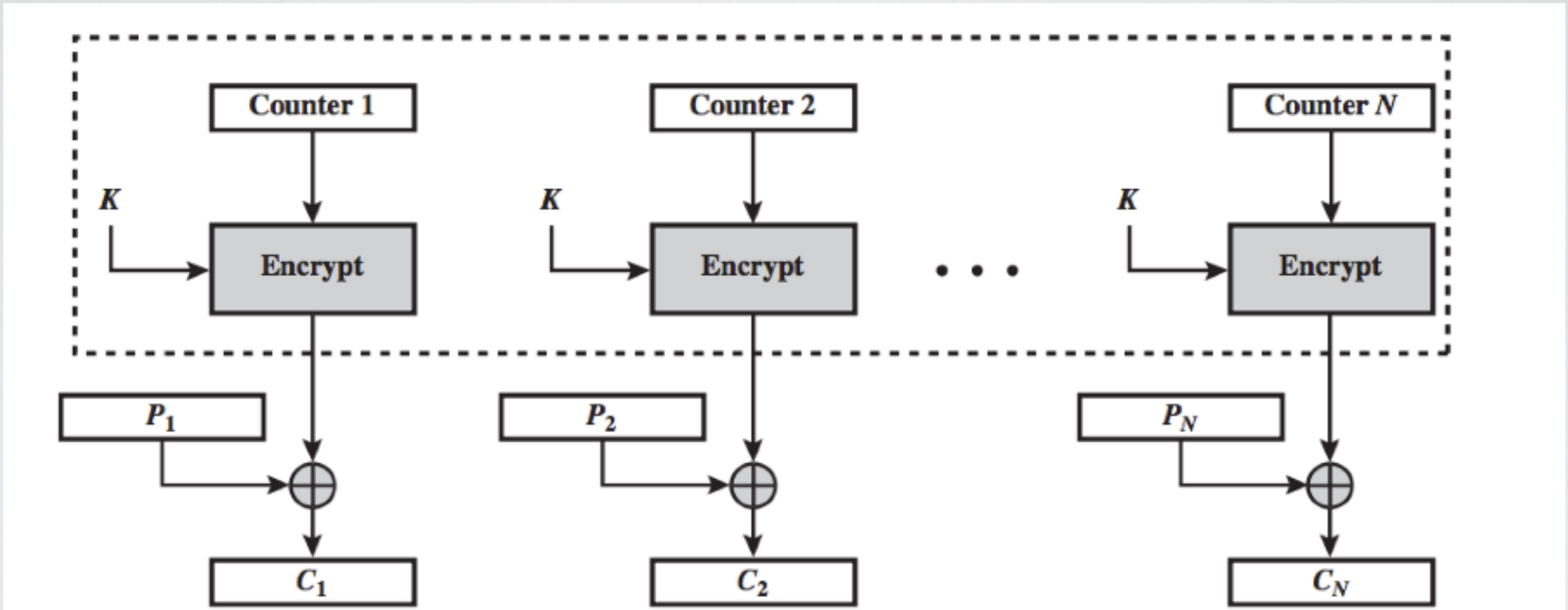
CBC - Cipher Block Chaining



Introduce some <u>randomness</u> using the previous ciphertext block

- ✓ Repeating plaintext blocks are not exposed in the ciphertext
- ◉ No parallelism
- ➡ The Initialization Vector should not be known by the recipient

CTR - Counter



Introduce some <u>randomness</u> using a counter

- ✓ High entropy and parallelism
- ◉ Sensitive to key-reused attack