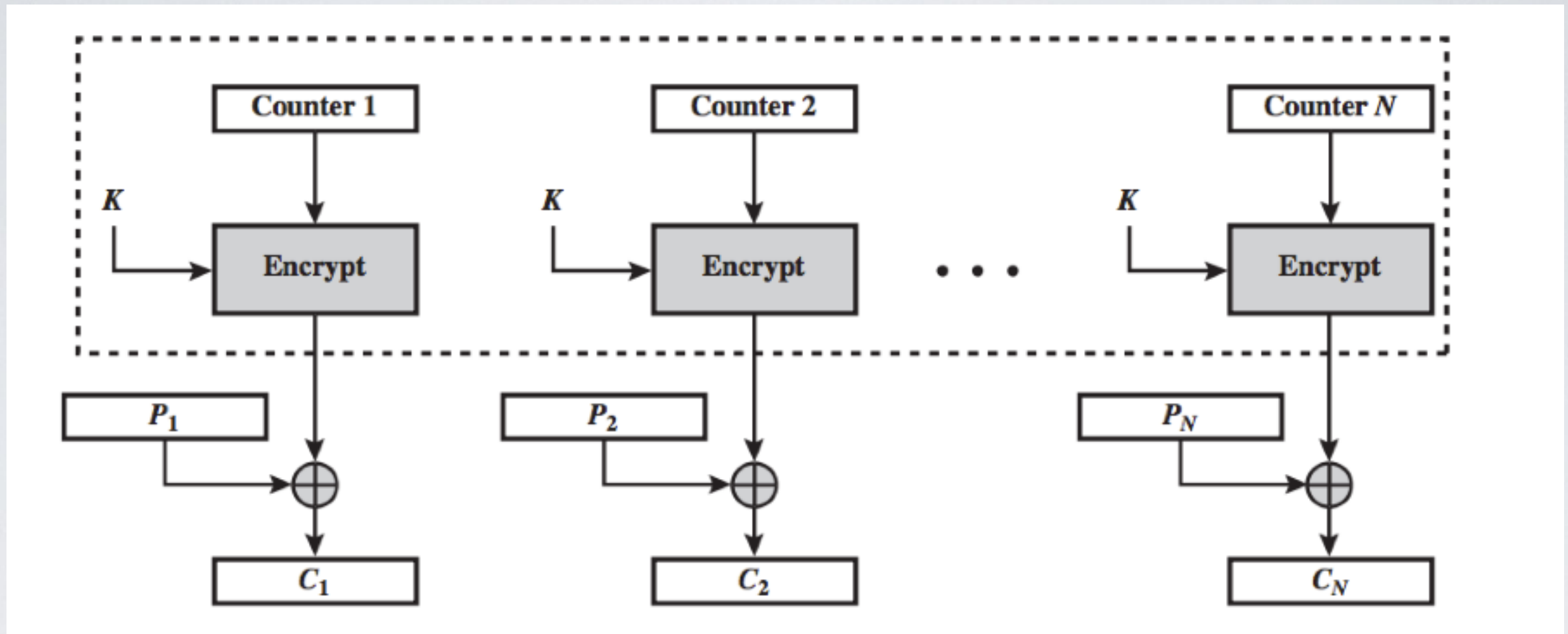


# CTR - Counter



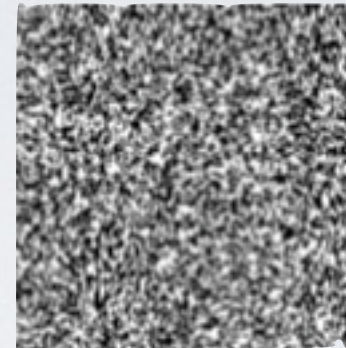
Introduce some randomness using a counter

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

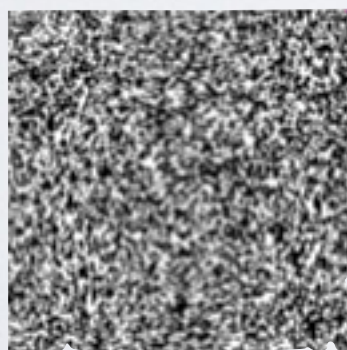
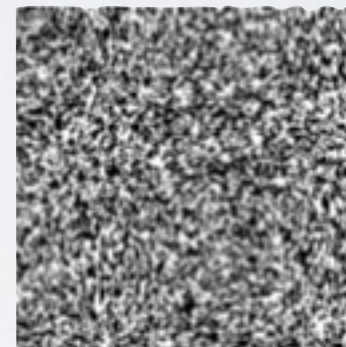
# Key-reused attack on CTR



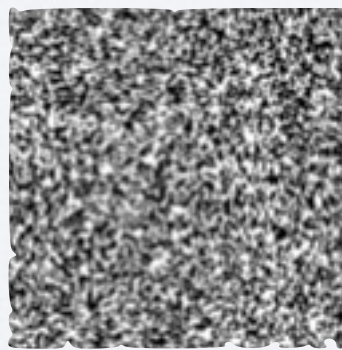
$$\oplus K =$$



$$\oplus K =$$



$$\oplus$$



$$=$$

