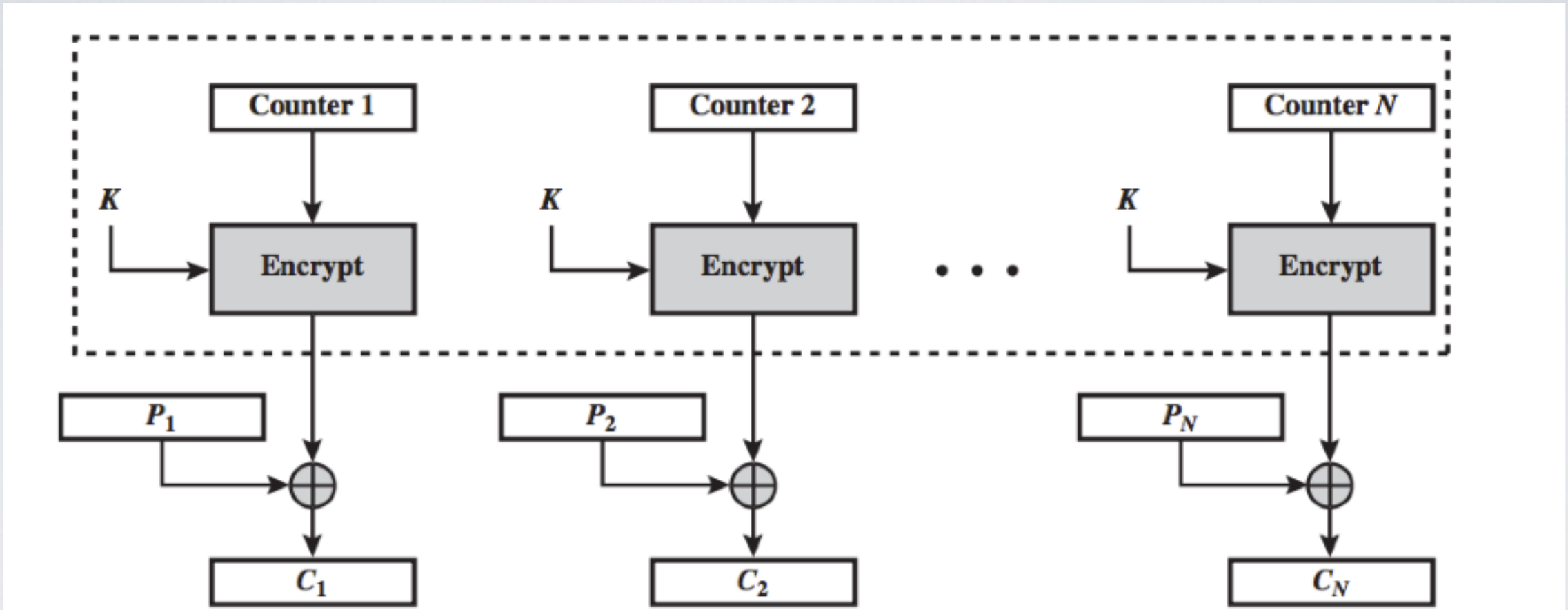
CTR - Counter Mode

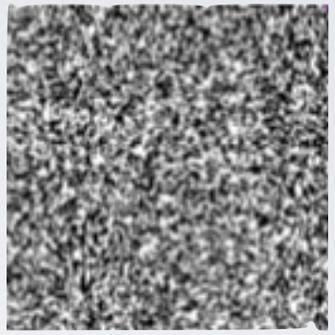


Introduce some randomness using a counter

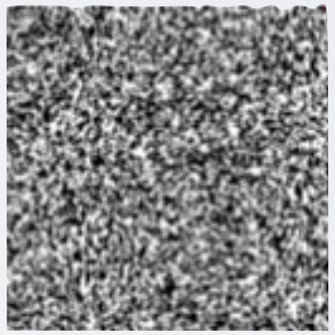
- ✓ High entropy and parallelism
- ◉ Behaves as a stream cipher - sensitive to key-reused attack

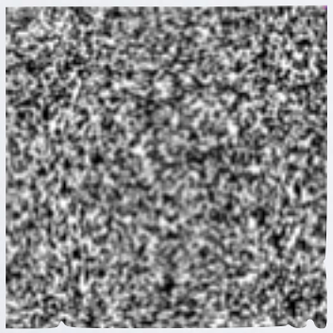
Key-reused attack on CTR

$\oplus$ K =

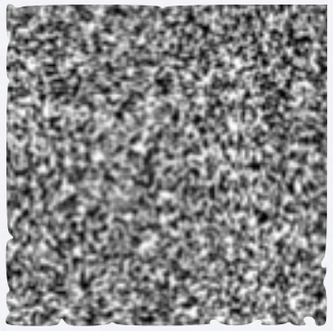


$\oplus$ K =





$\oplus$



=