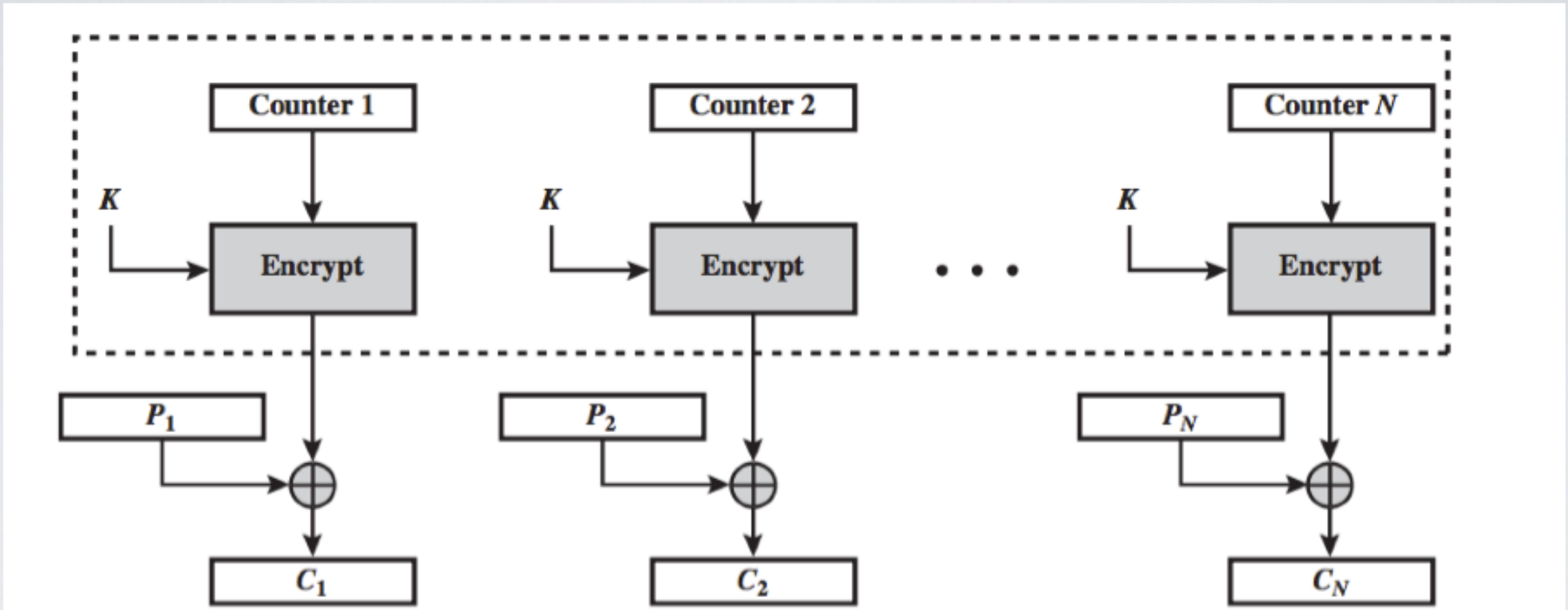
CTR - Counter

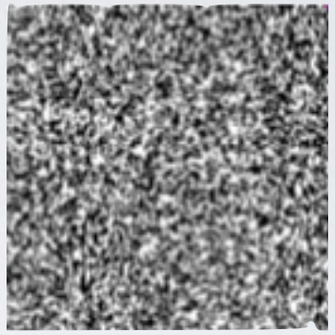


Introduce some randomness using a counter

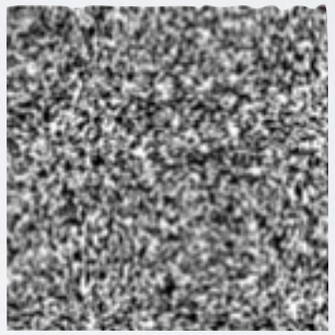
- ✓ High entropy and parallelism
- ◉ Sensitive to key-reused attack
- ➡ Popular usage : IPsec (coming soon in this course)

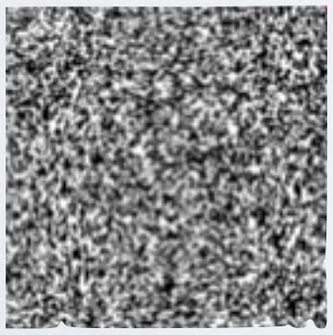
Key-reused attack on CTR

$\oplus$ K =

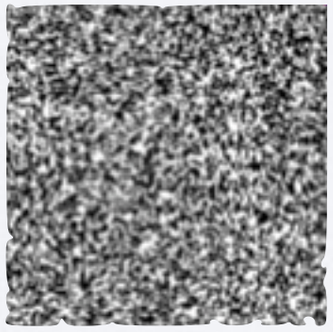


$\oplus$ K =





$\oplus$



=