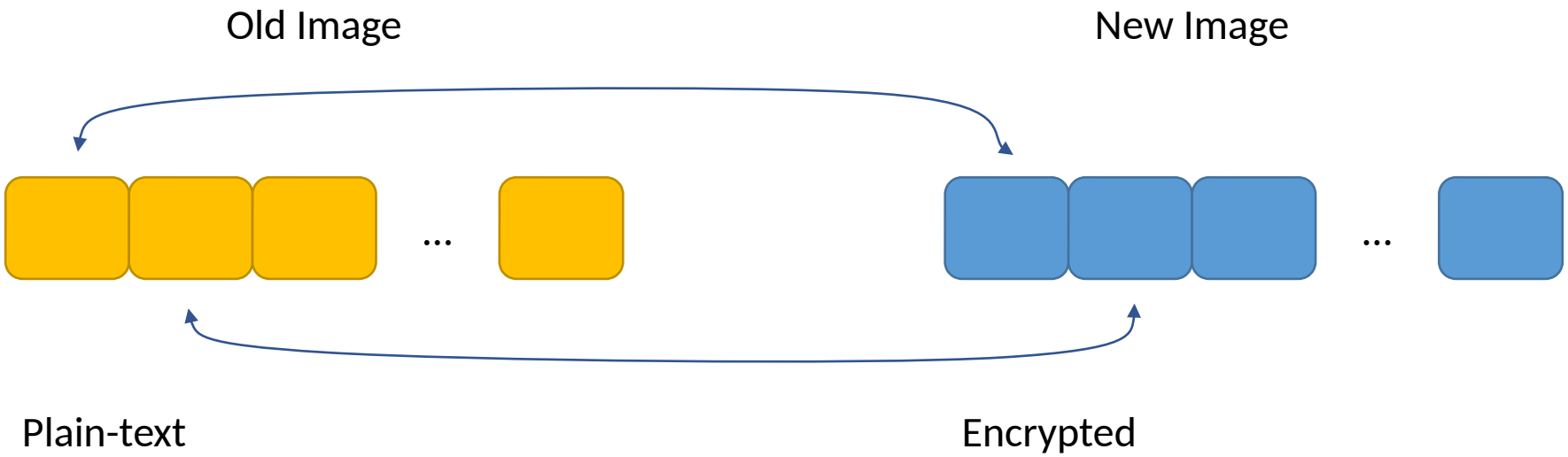
Firmware Encryption with SUIT Manifests

Encrypted Firmware Upgrade



- Both images in flash
- Insufficient RAM to hold entire image
- Exchanged one block at a time
- New image decrypted 1 block at a time
- Old image encrypted 1 block at a time

Constraints

- Update can be interrupted (power loss, etc)
- Need to be restarted when power is restored
- Typically use something like AES-CTR

AEAD vs Update

AEAD

- Tag covering whole image
- Must encrypt/decrypt whole image
- Ensures integrity of whole image

Firmware Update

- No space for per-block tag
- CTR mode can be done per block
- Rely on signature covering whole image

Needed for SUIT

- COSE to consider allowing unauthenticated encryption
- May have a clause requiring integrity
- Upgrade verifies signature over plaintext before running
- Upgrade may verify signature by decrypting to temporary buffer, to avoid flash wear on invalid image