Authenticated Encryption with Replay prOtection (AERO)

mcgrew@cisco.com

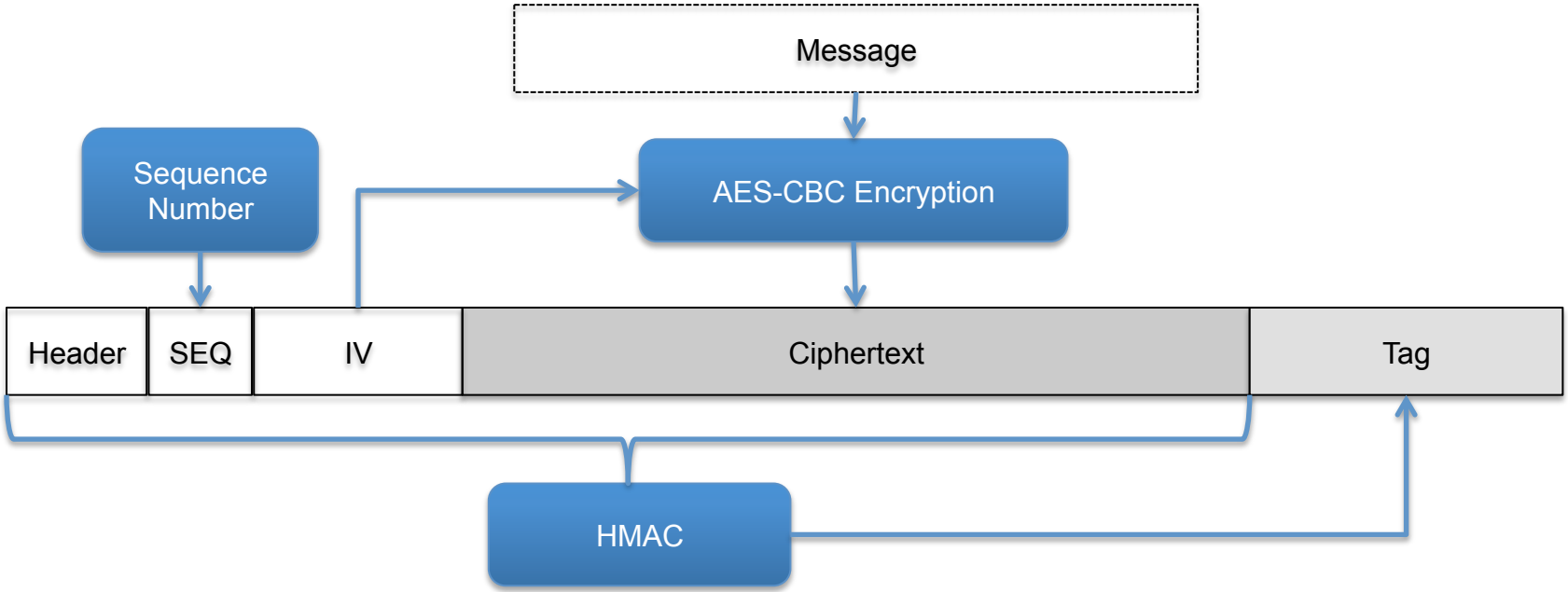
AERO

- Authenticated Encryption algorithm
- Stateful and self-synchronizing
- Easy to use
- Robust against nonce misuse and decryption misuse
- Saves bandwidth
  - No nonce, no sequence number
- New standards contributions and research

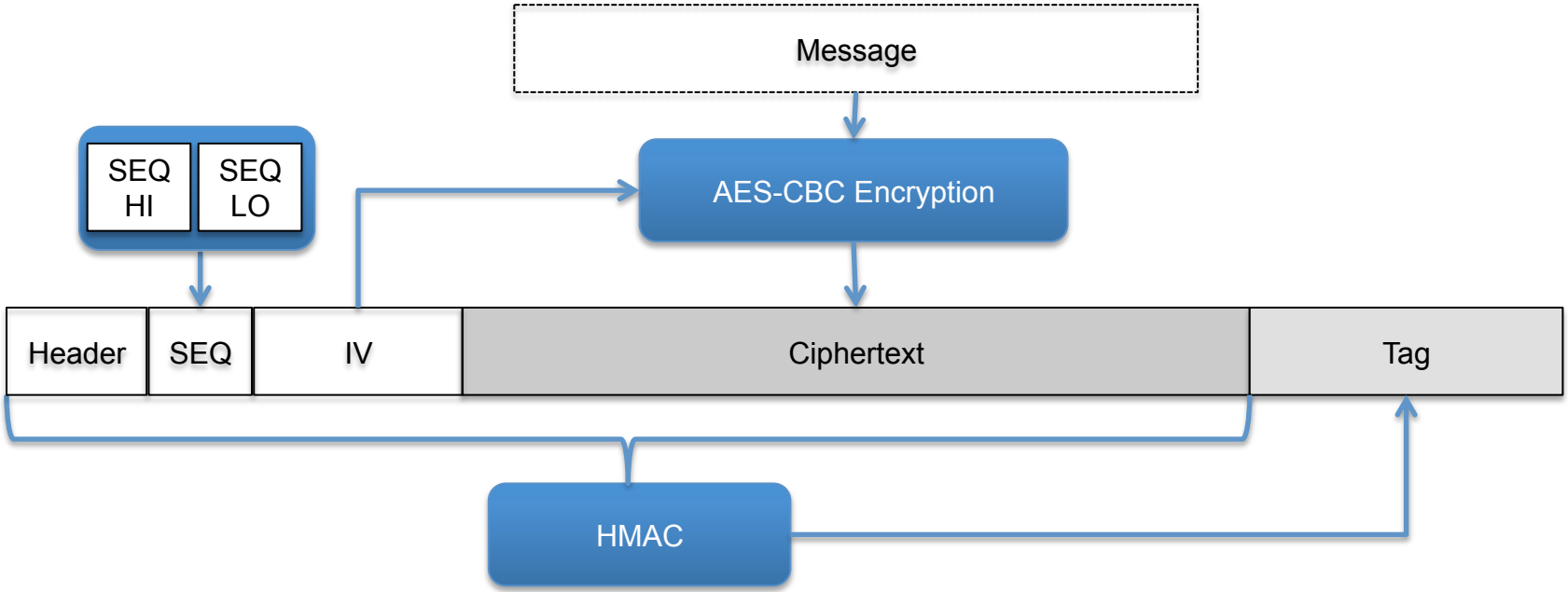
Communication Security Goals

- Unreliable transport
  - Message loss
  - Message reorder
- Multiple senders, multiple receivers
- Adaptive chosen plaintext, chosen ciphertext attacks
  - Security against forgery
  - Plaintext indistinguishable from random

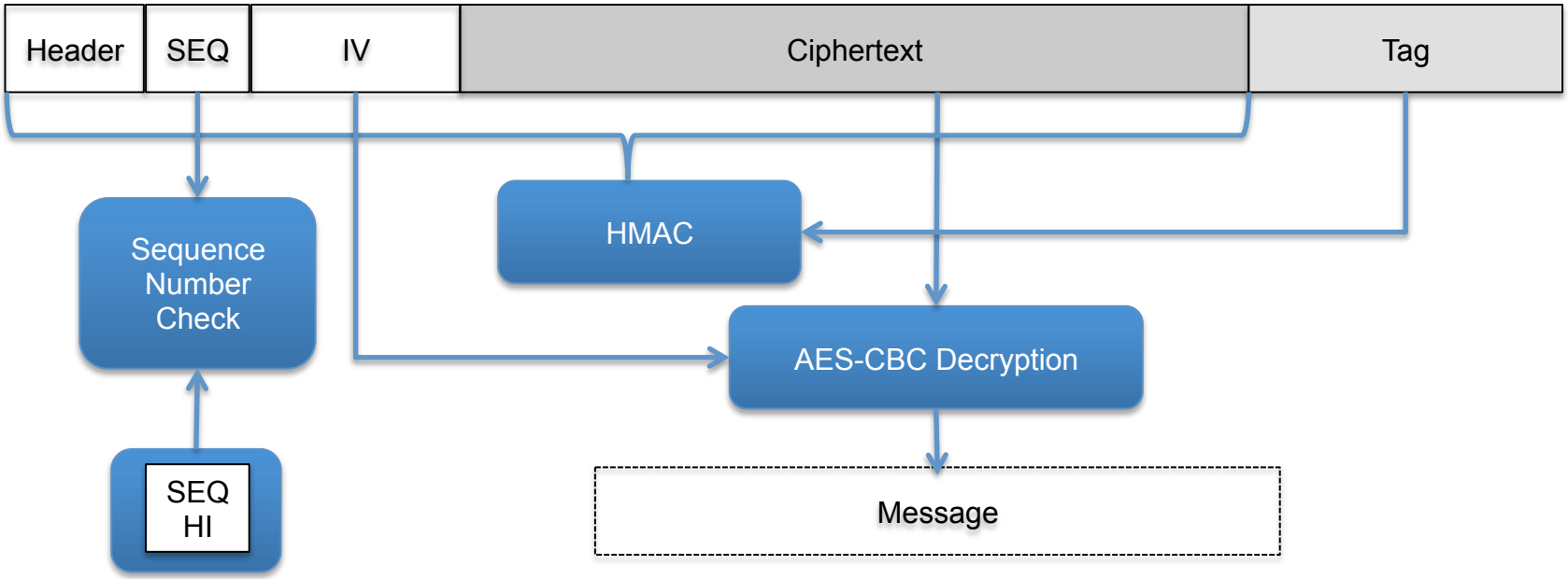
Conventional Encryption + Authentication



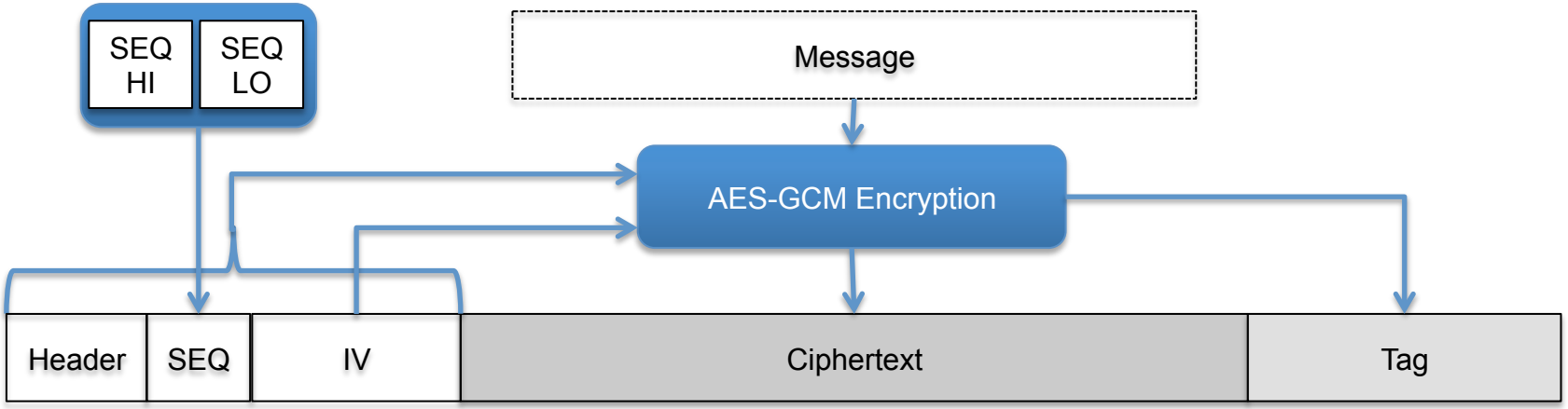
Conventional A+E with Extended SEQ



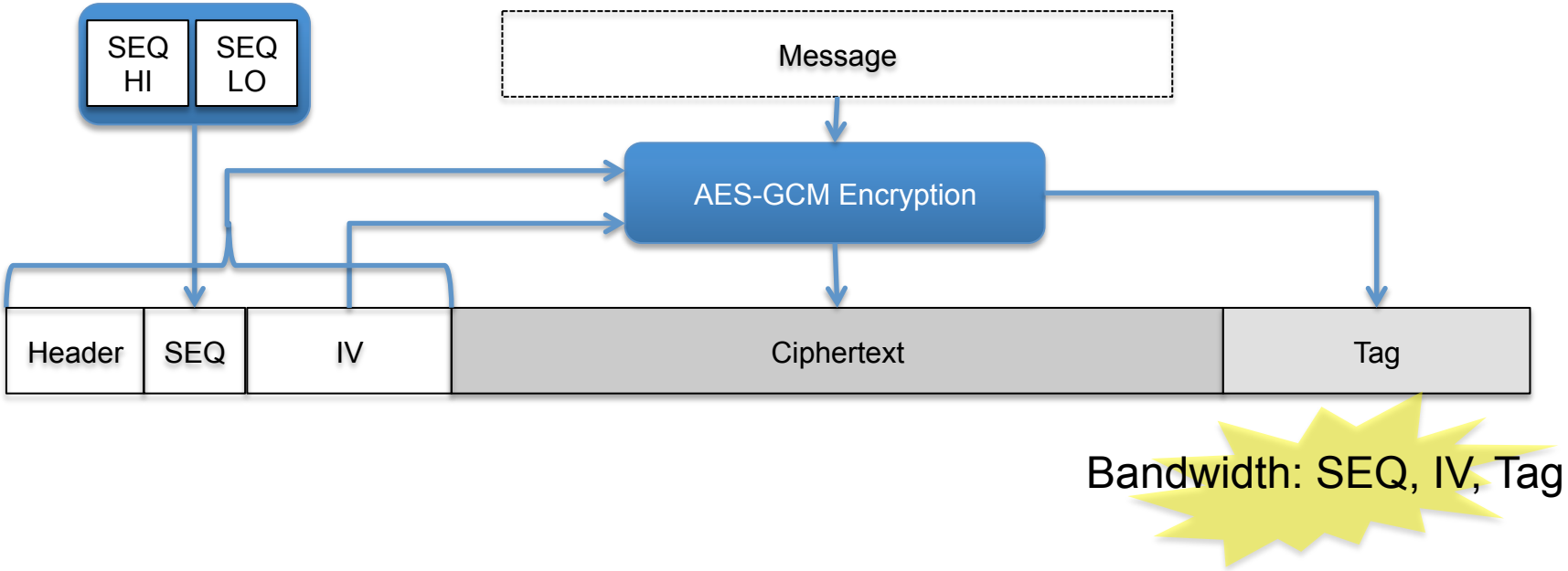
Conventional Decryption



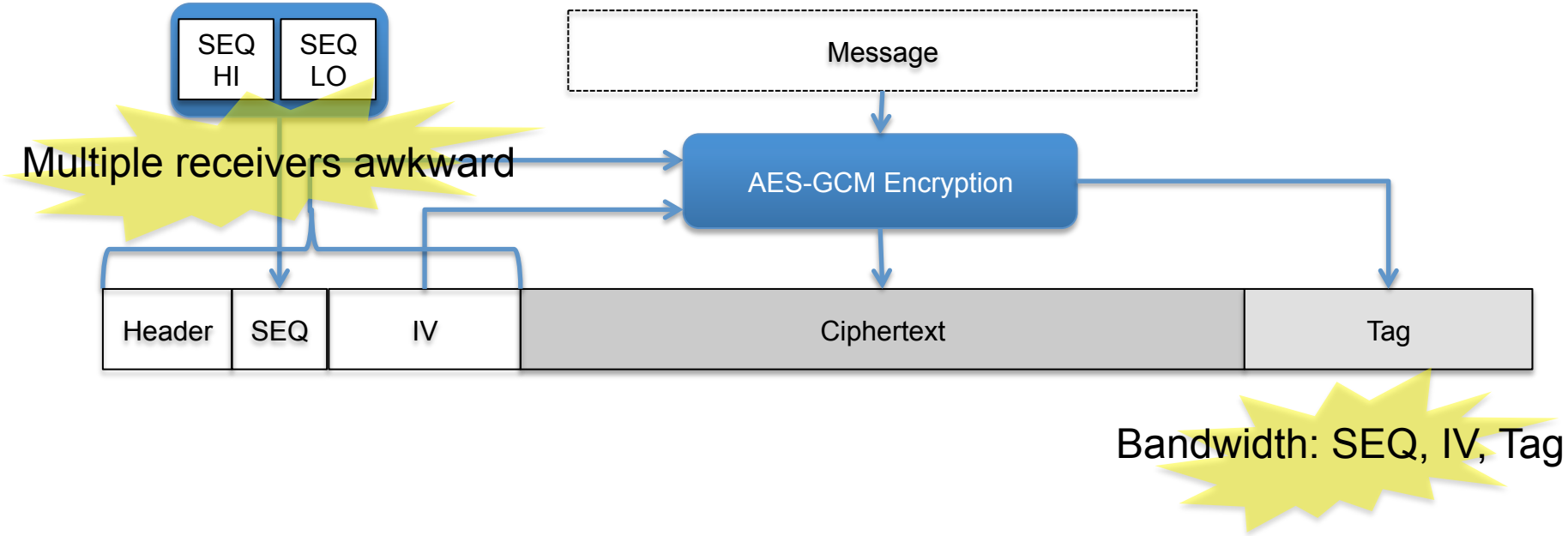
Authenticated Encryption with Associated Data (AEAD)



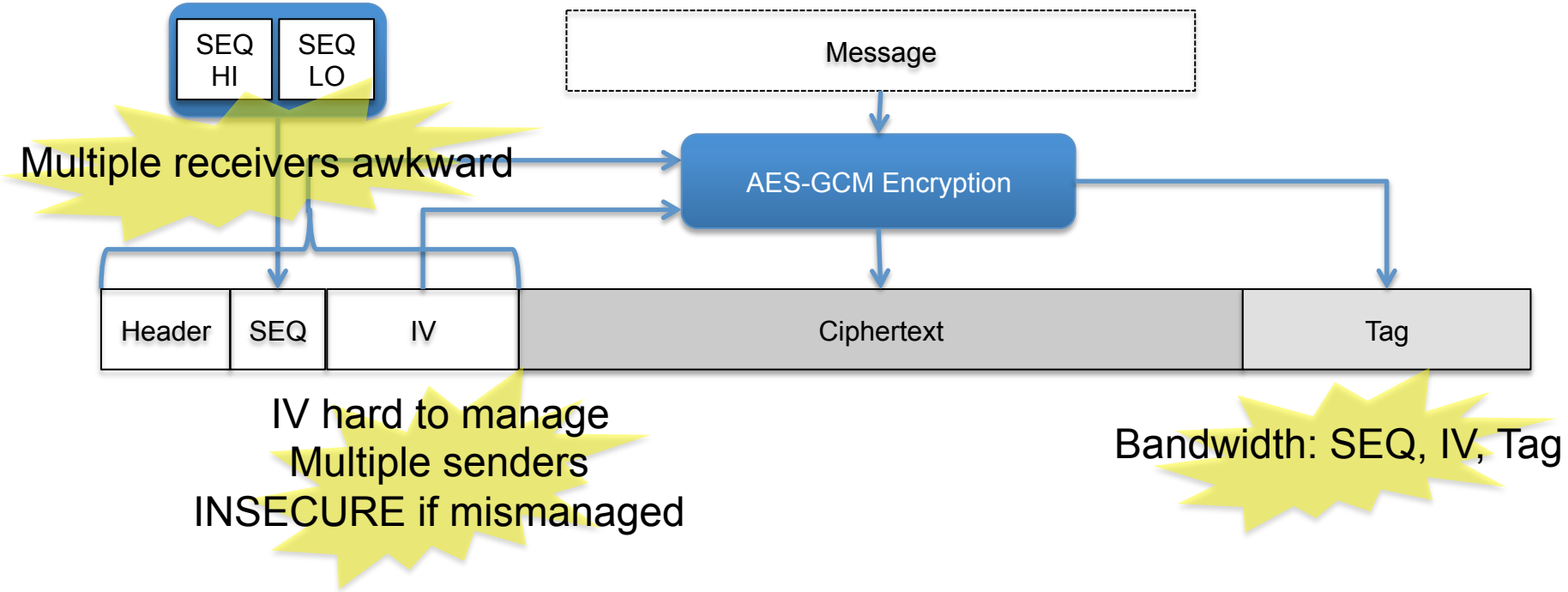
Authenticated Encryption with Associated Data (AEAD)



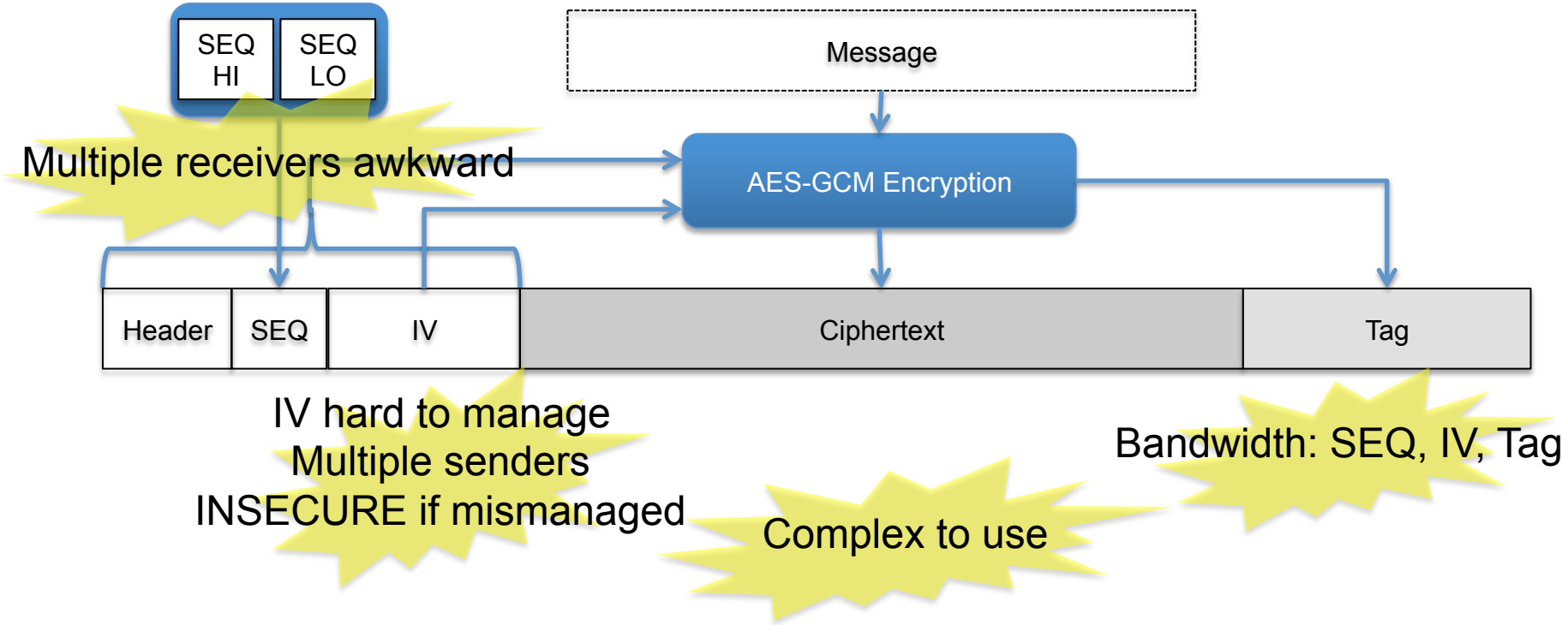
Authenticated Encryption with Associated Data (AEAD)



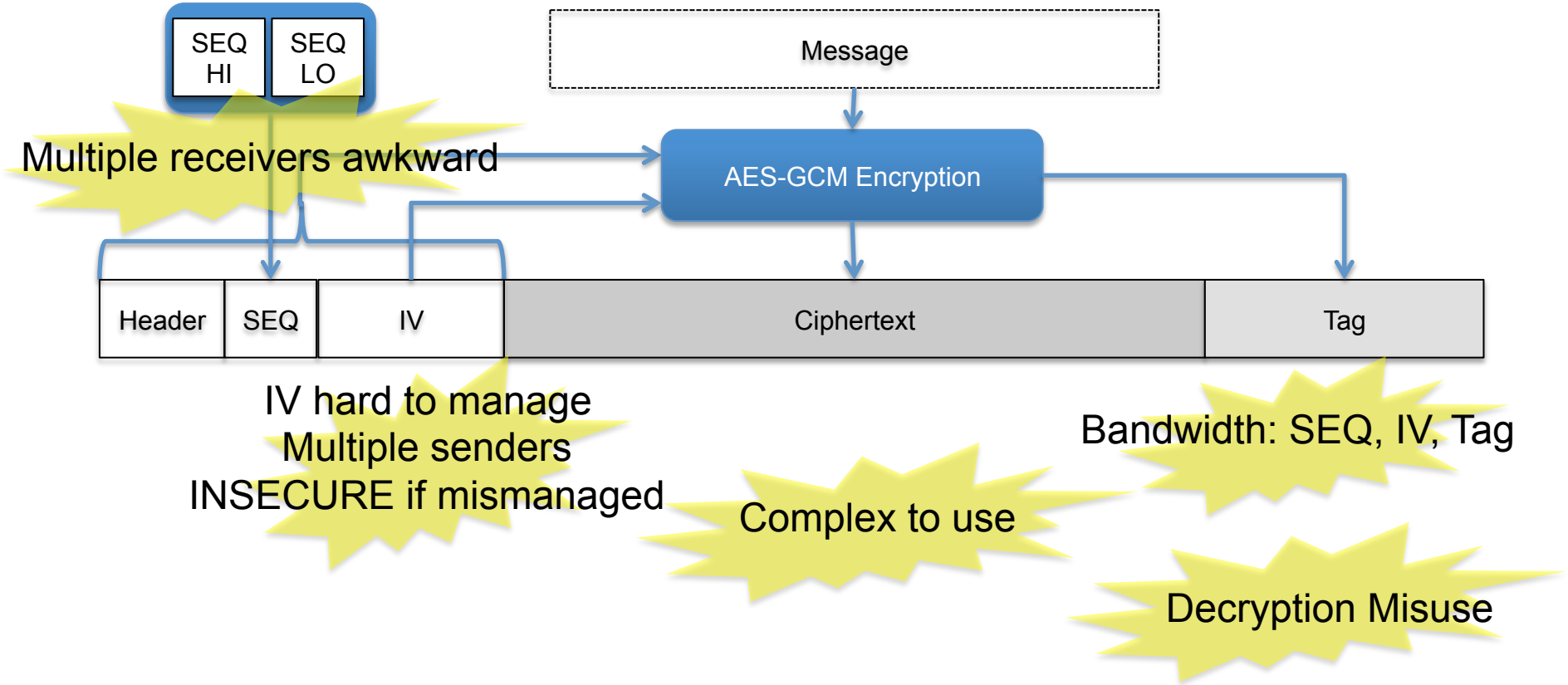
Authenticated Encryption with Associated Data (AEAD)



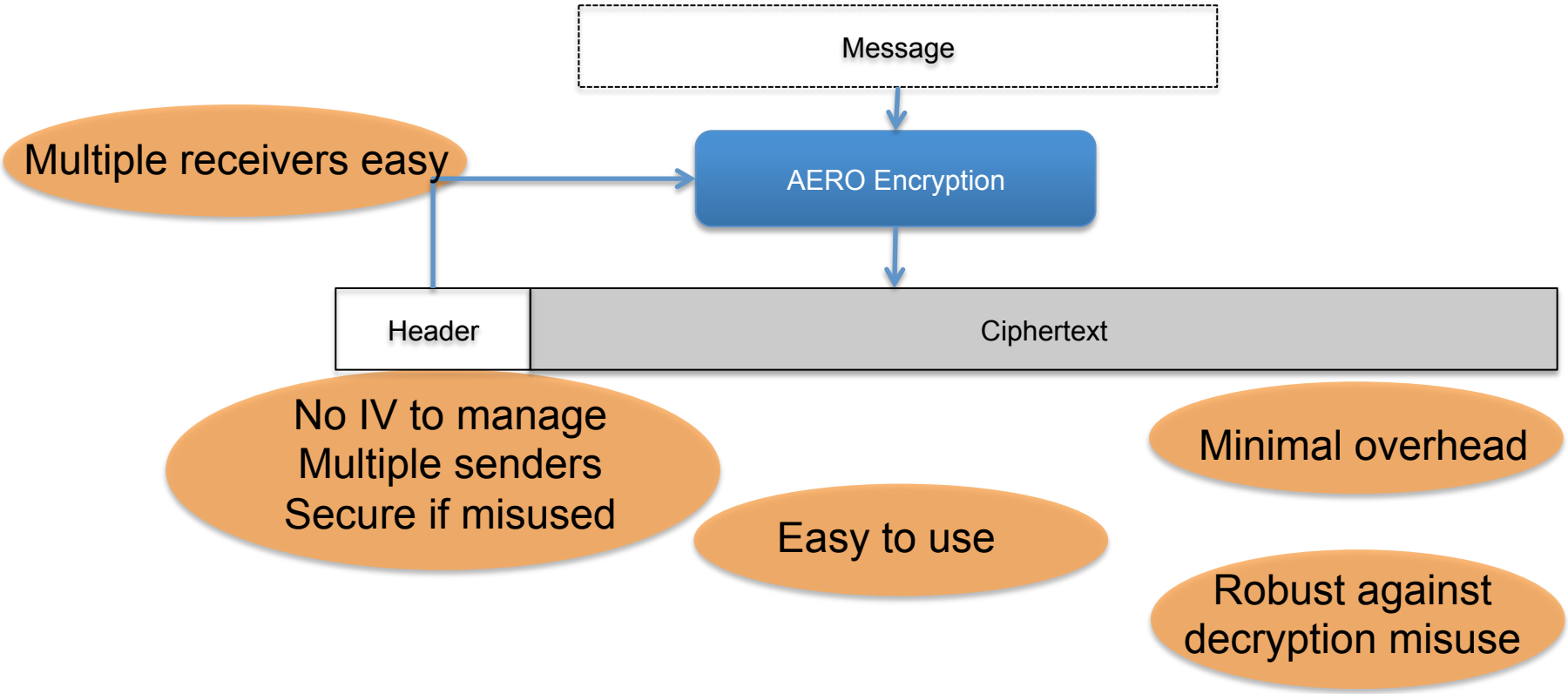
Authenticated Encryption with Associated Data (AEAD)



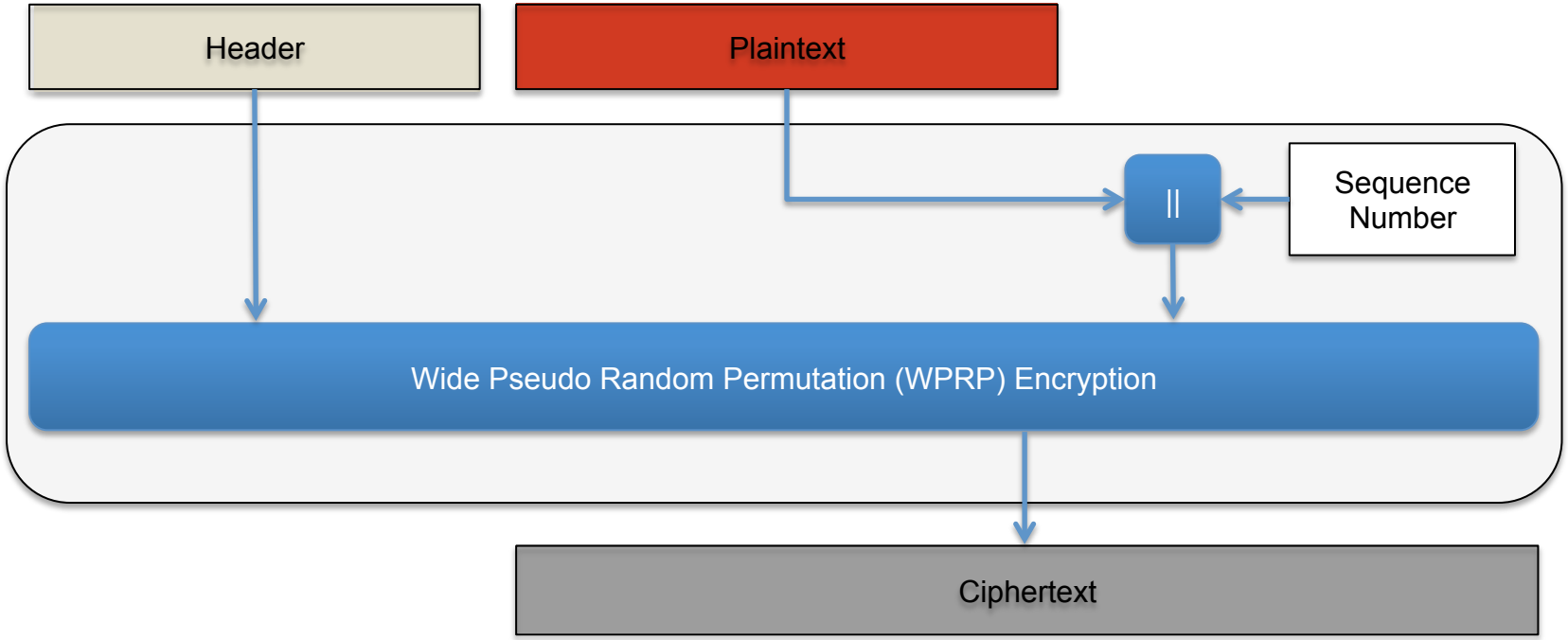
Authenticated Encryption with Associated Data (AEAD)



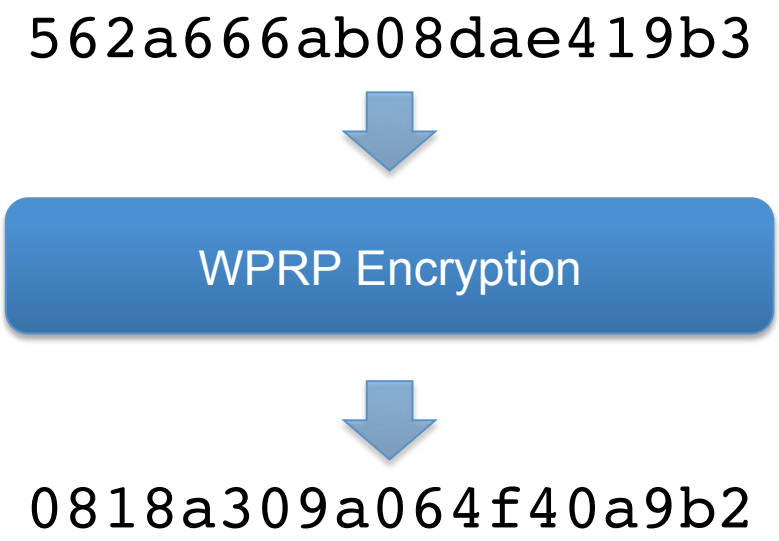
AERO


Message
Multiple receivers easy
AERO Encryption
Header
Ciphertext
No IV to manage
Multiple senders
Secure if misused
Minimal overhead
Easy to use
Robust against
decryption misuse

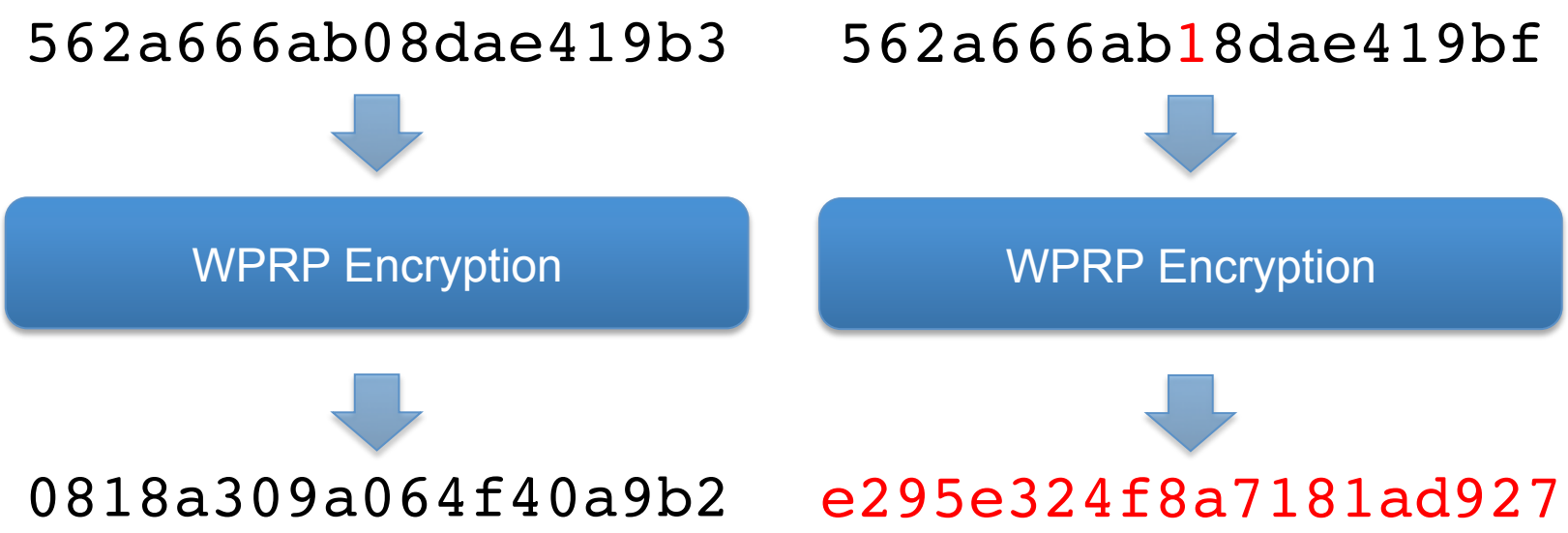
AERO Encryption



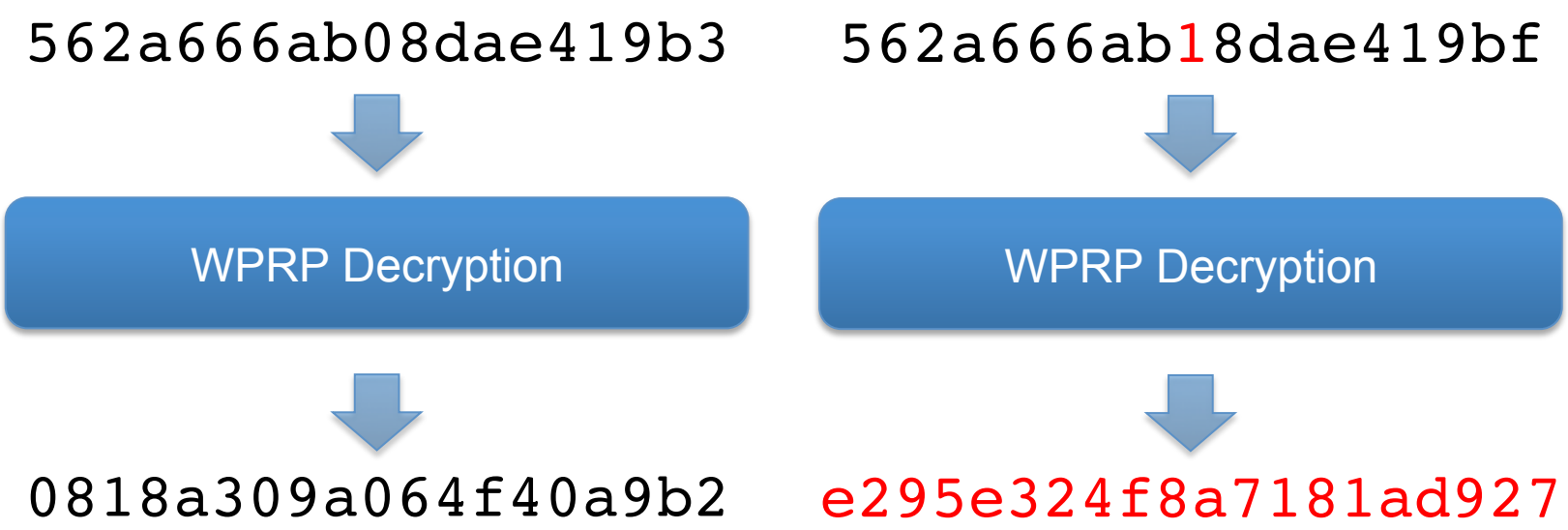
Wide Pseudo Random Permutation (WPRP)



Wide Pseudo Random Permutation (WPRP)

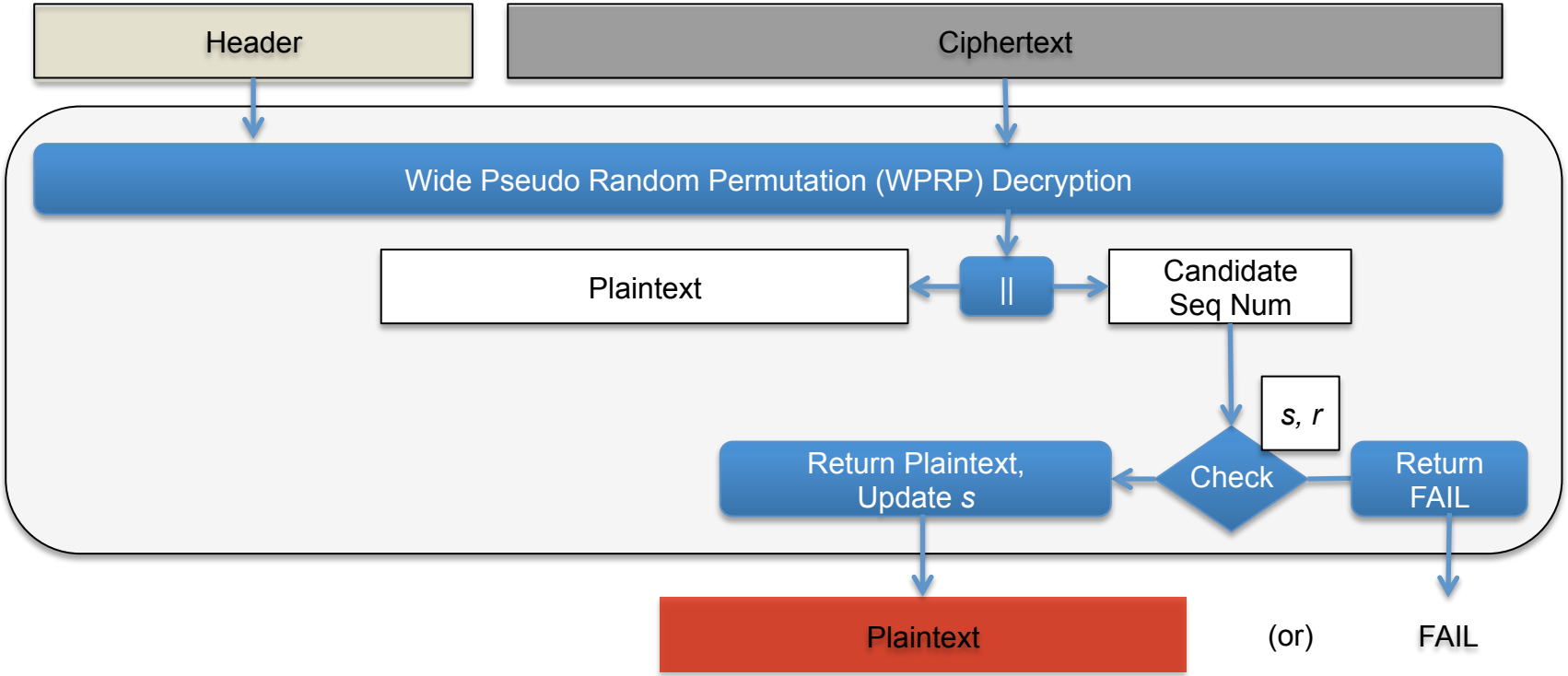


Wide Pseudo Random Permutation (WPRP)

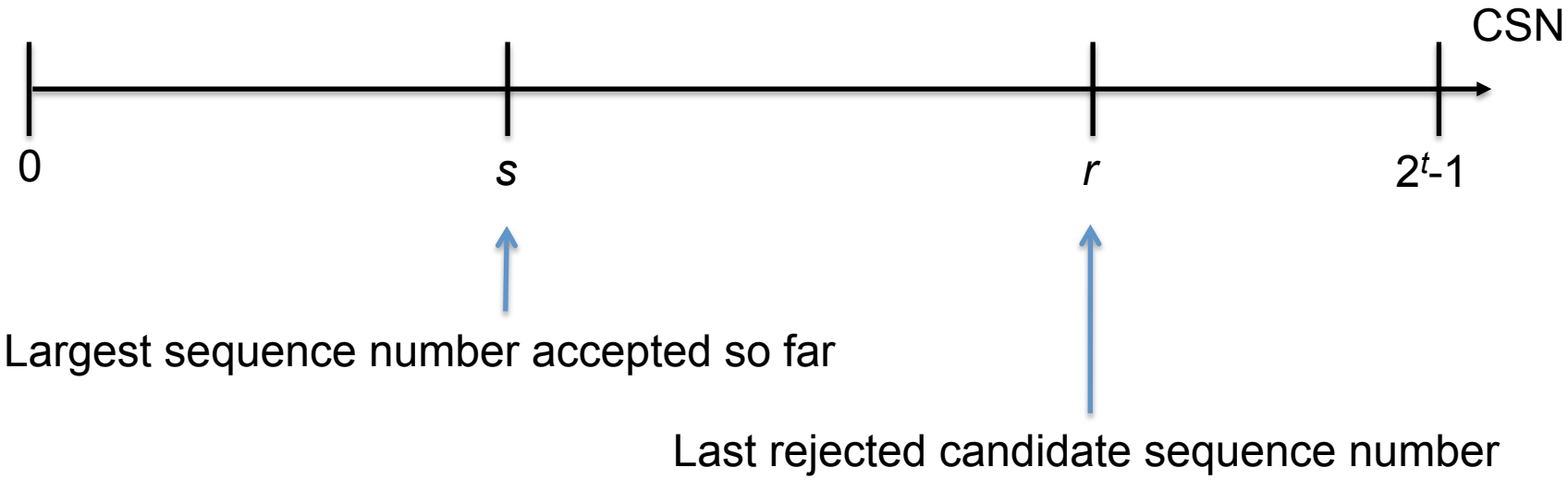


AES Extended Codebook (XCB) Mode of Operation

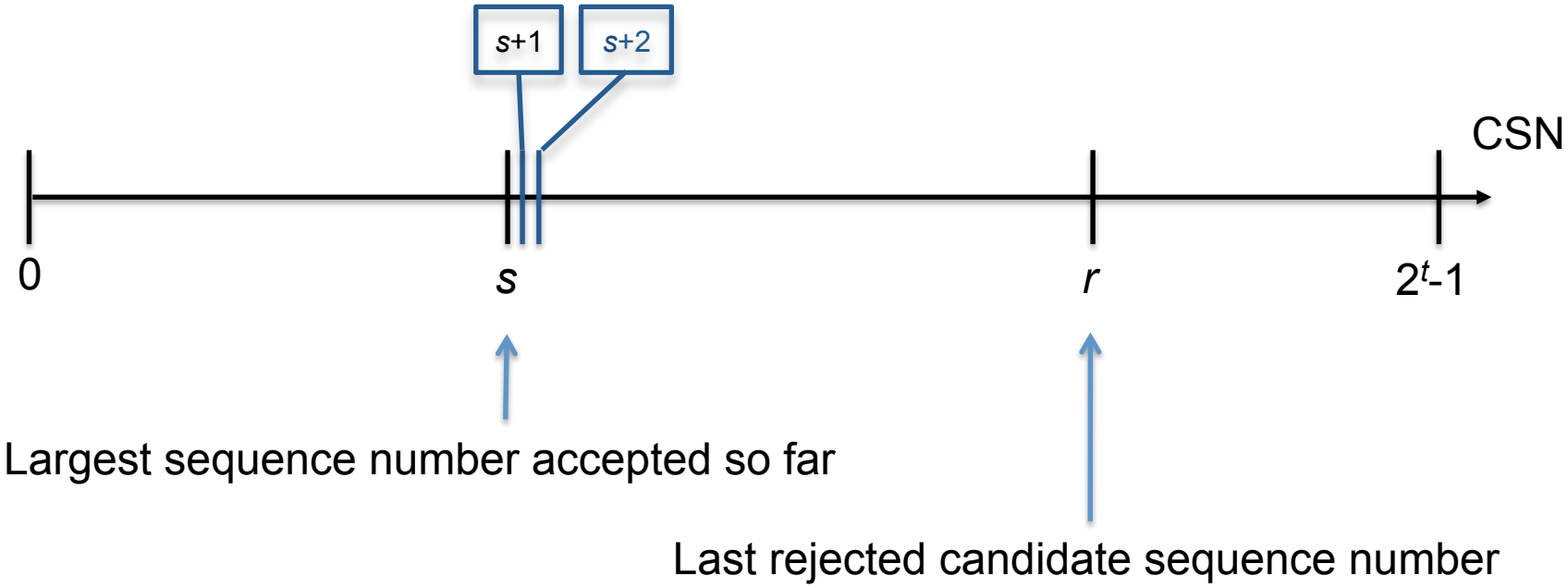
AERO Decryption



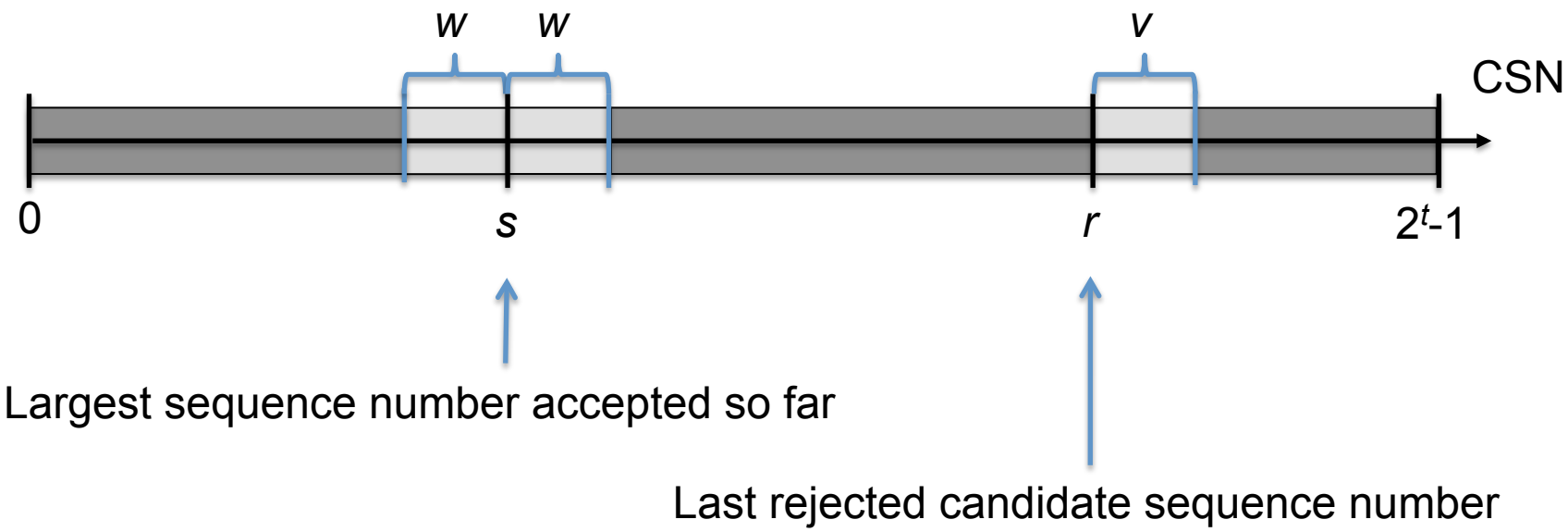
Candidate Sequence Number Checking



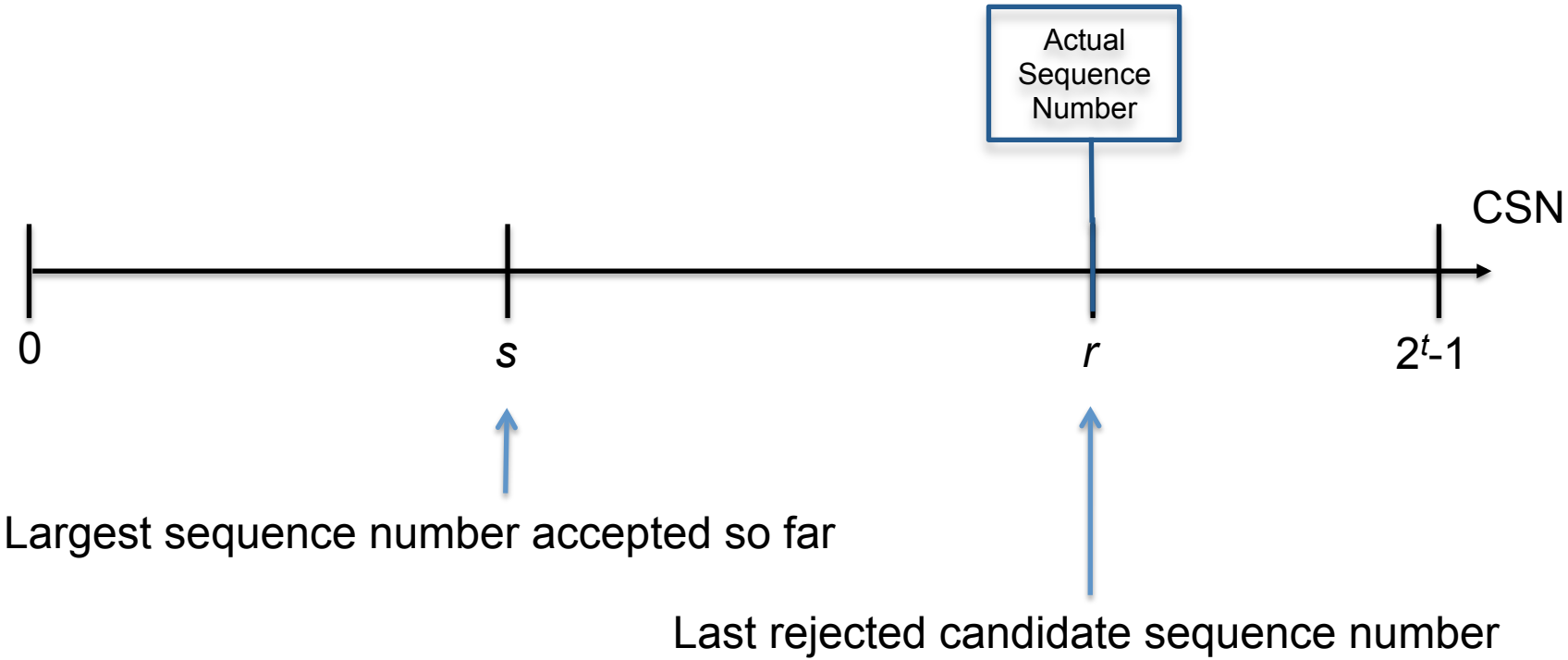
Likely next candidates



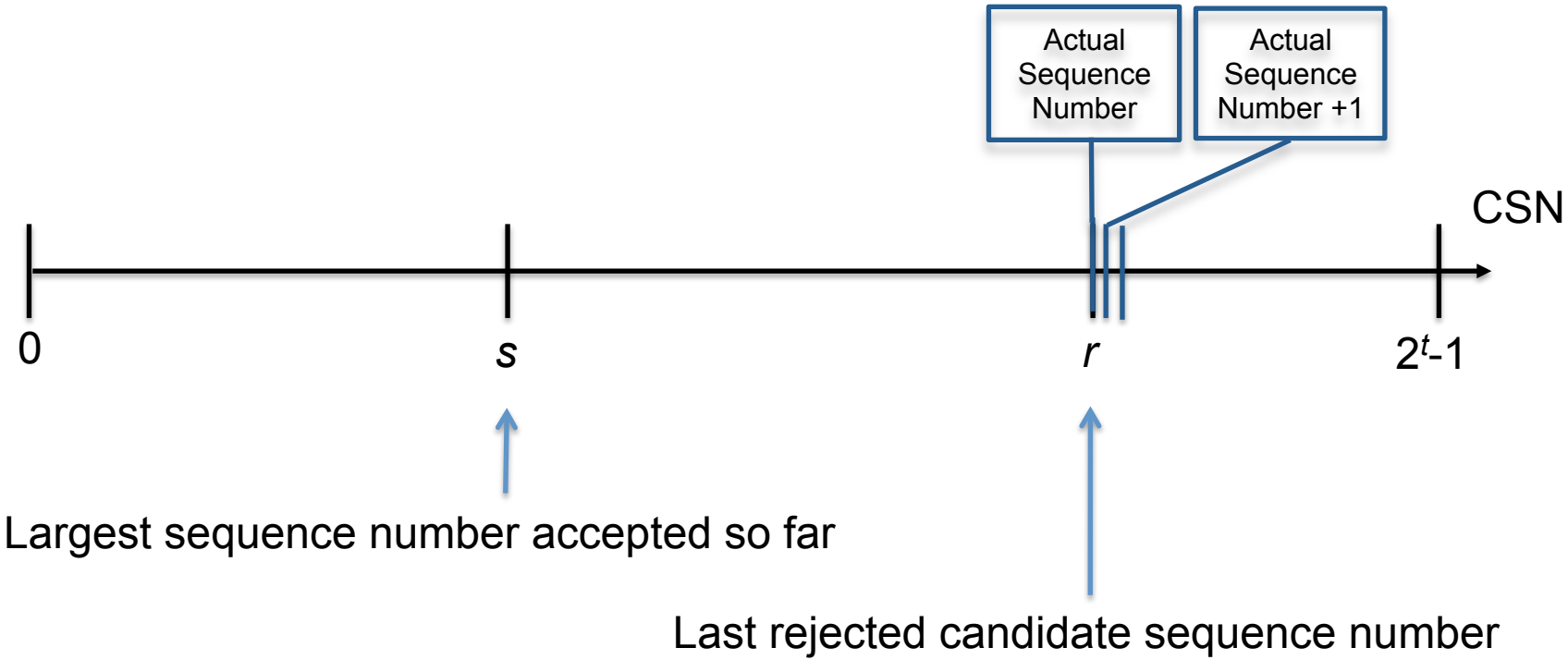
Candidate Sequence Number Checking



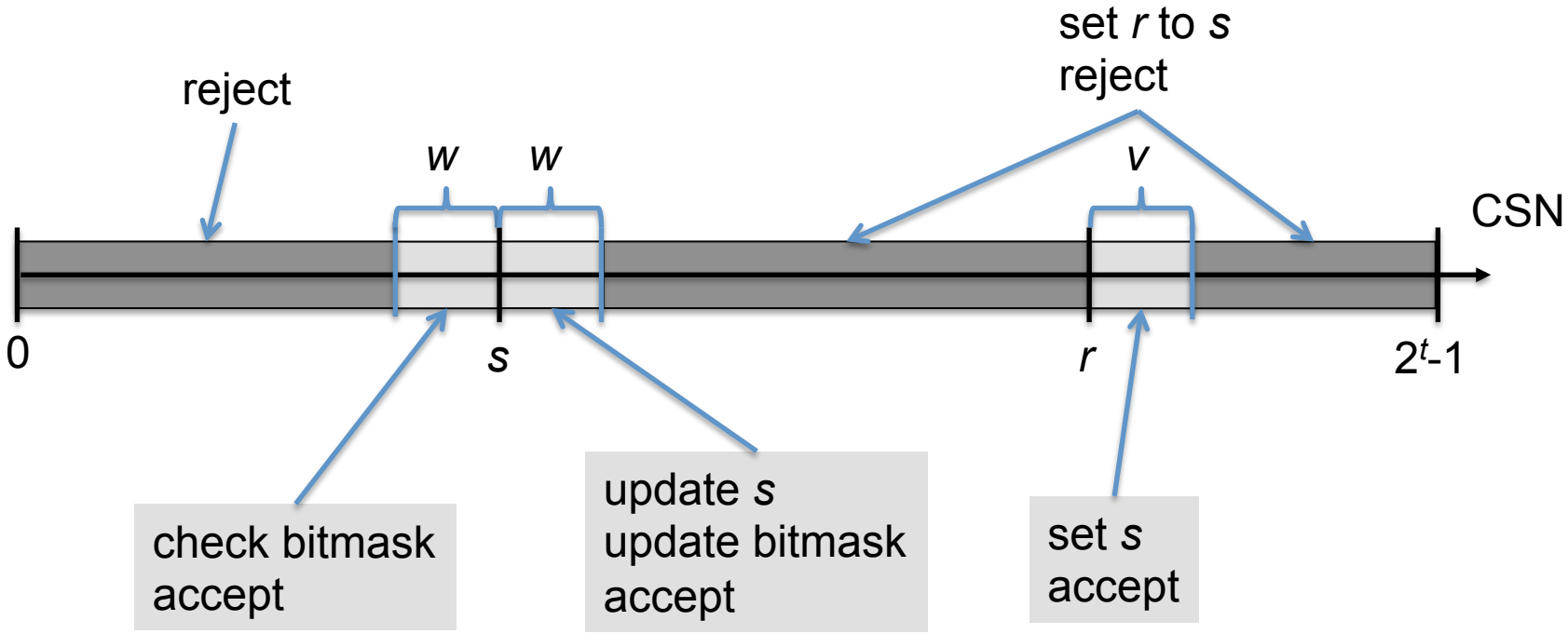
(Re)synchronization



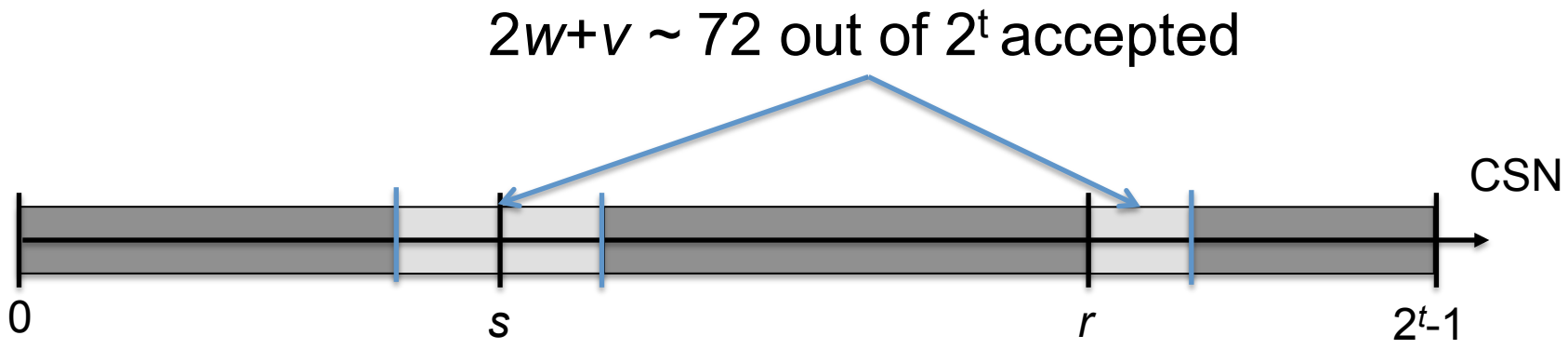
(Re)synchronization



Candidate Sequence Number Checking



Security of Authentication



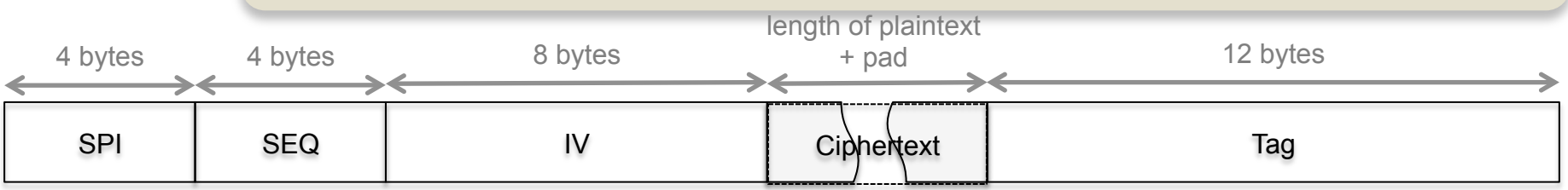
Probability of successful forgery $= \frac{72}{2^t} \sim 2^{-t+7}$

IPSec

ESP AES-GCM, AES-CCM, or AES-CTR plus HMAC-SHA1

no misuse resistance

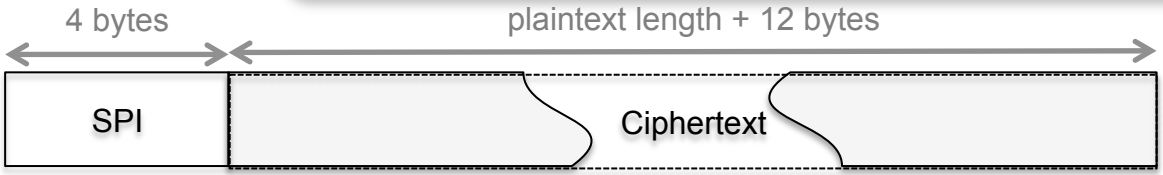
24+ bytes overhead per packet



ESP AERO

misuse resistance

12 bytes overhead per packet



Performance

- WPRP CPB ~ 1.5 x GCM CPB
- Inefficient on long messages
  - Higher latency
  - Larger memory requirements
  - … but this is true of *all* AEAD methods …
- More efficient on short messages
  - Short frames (about 100 bytes for 802.15)
    - Four bytes less overhead means:
    - ~ 4% less power used in transmission
    - ~ 4% less power used in reception
    - ~ 4% lower probability that retransmission is needed

Status

- Research
  - Formalization of security models and goals
  - WPRP encryption alternatives
- IETF
  - `draft-mcgrew-aero-00.txt`
  - `draft-mcgrew-srtp-aero-01.txt`
  - `draft-mcgrew-dtls-aero-00.txt`
- CAESAR
  - Does not work with conventional AEAD API