Low power wireless scenarios and techniques for saving bandwidth without sacrificing security

David McGrew, PhD
Cisco Fellow
mcgrew@cisco.com

Low power wireless

Wireless and IoT

802.15.4: ZigBee, 6LoWPAN
LoRaWAN
Bluetooth
WiFi

Data encryption, JOSE, CMS, TLS, IPsec

Power cost

- Cost of transmission and reception often greater than cost of encryption and decryption
- Longer messages more likely to need retransmission

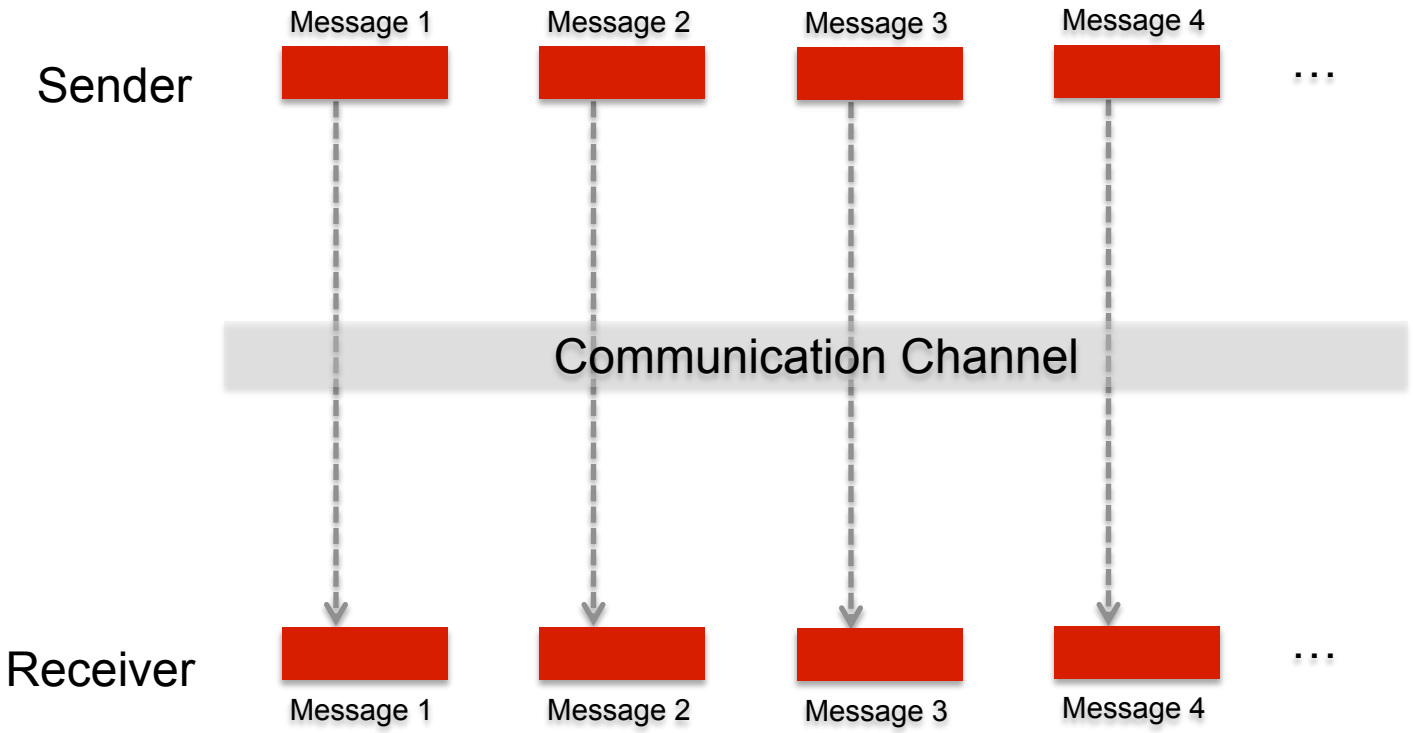
Seys and Preneel, WiMob 2005

Message and payload sizes

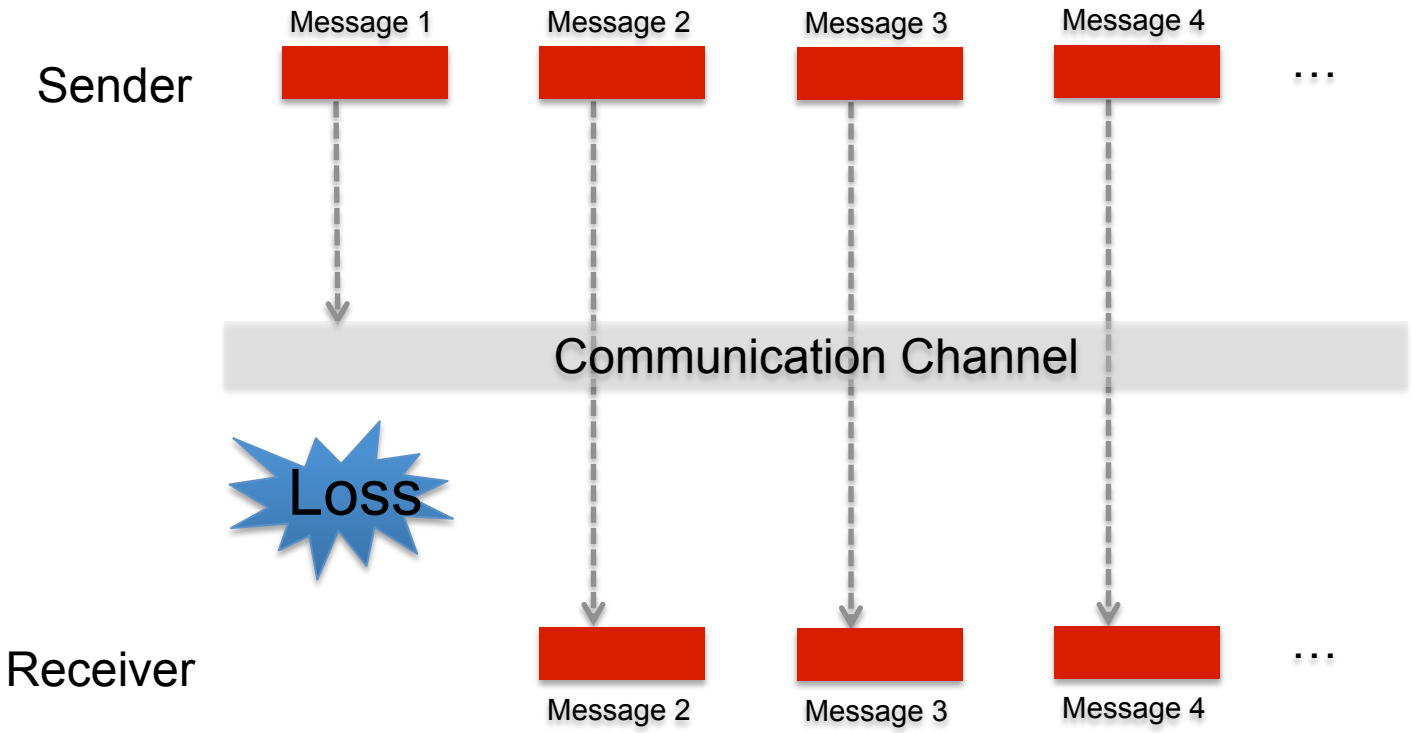
- Most 802.15.4g implementations limit 6LoWPAN to **800 bytes**
- Distributed Network Protocol DNP3 (IEEE Std 1815- 2010) has a maximum payload size of **292 bytes**
- LoRaWAN protocol supports packets up to **255 bytes**
  Includes operating modes for **11, 15, 129, and 242 bytes**
- ANSI C12.22, has plaintexts with an average size ranging from **64 to 600 bytes**

Communication Security

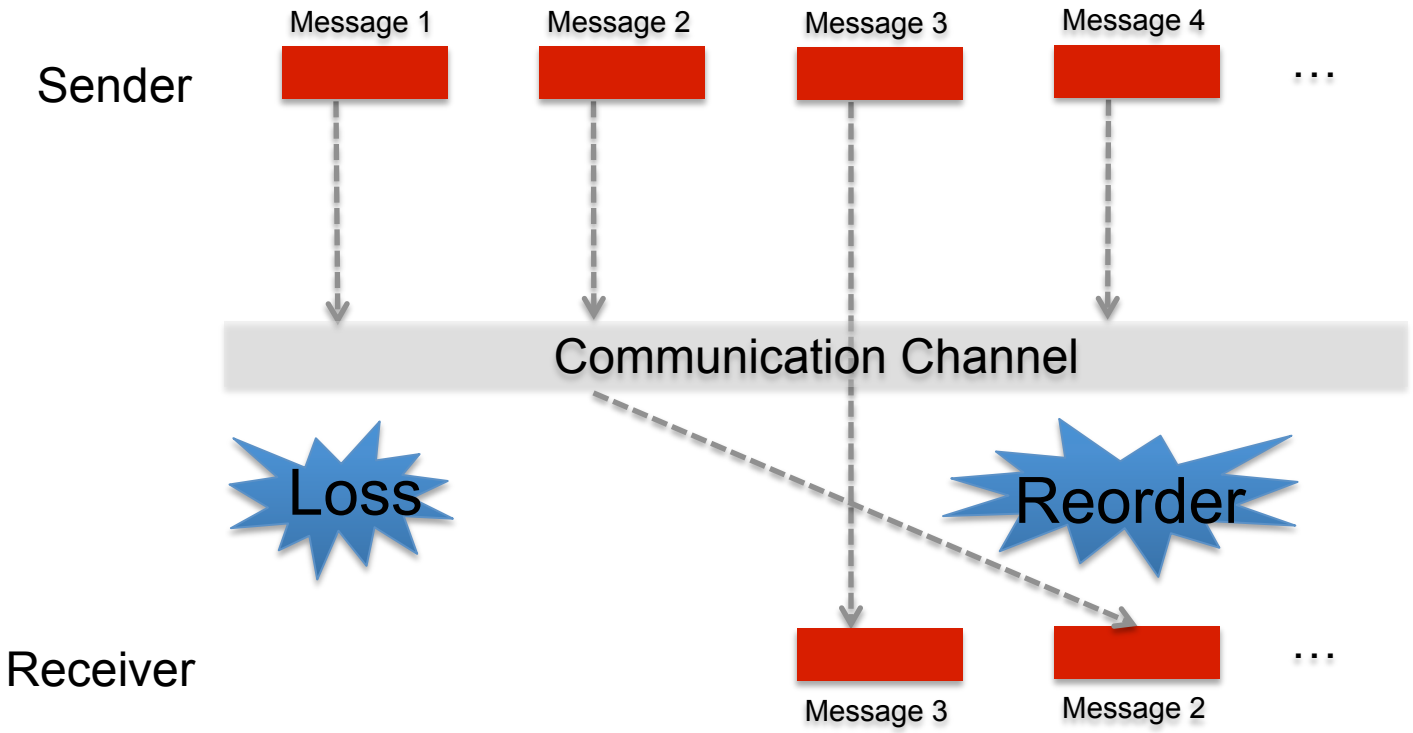
Unreliable Communication



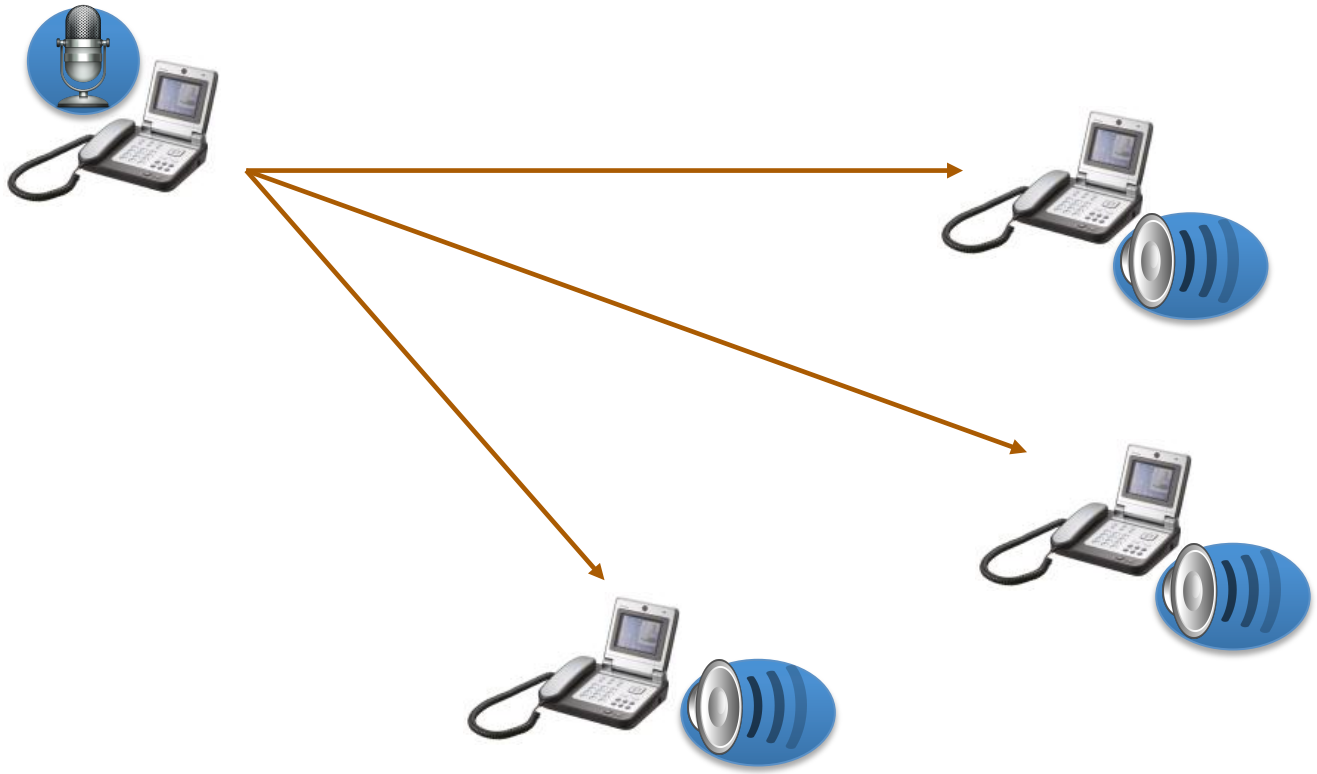
Unreliable Communication



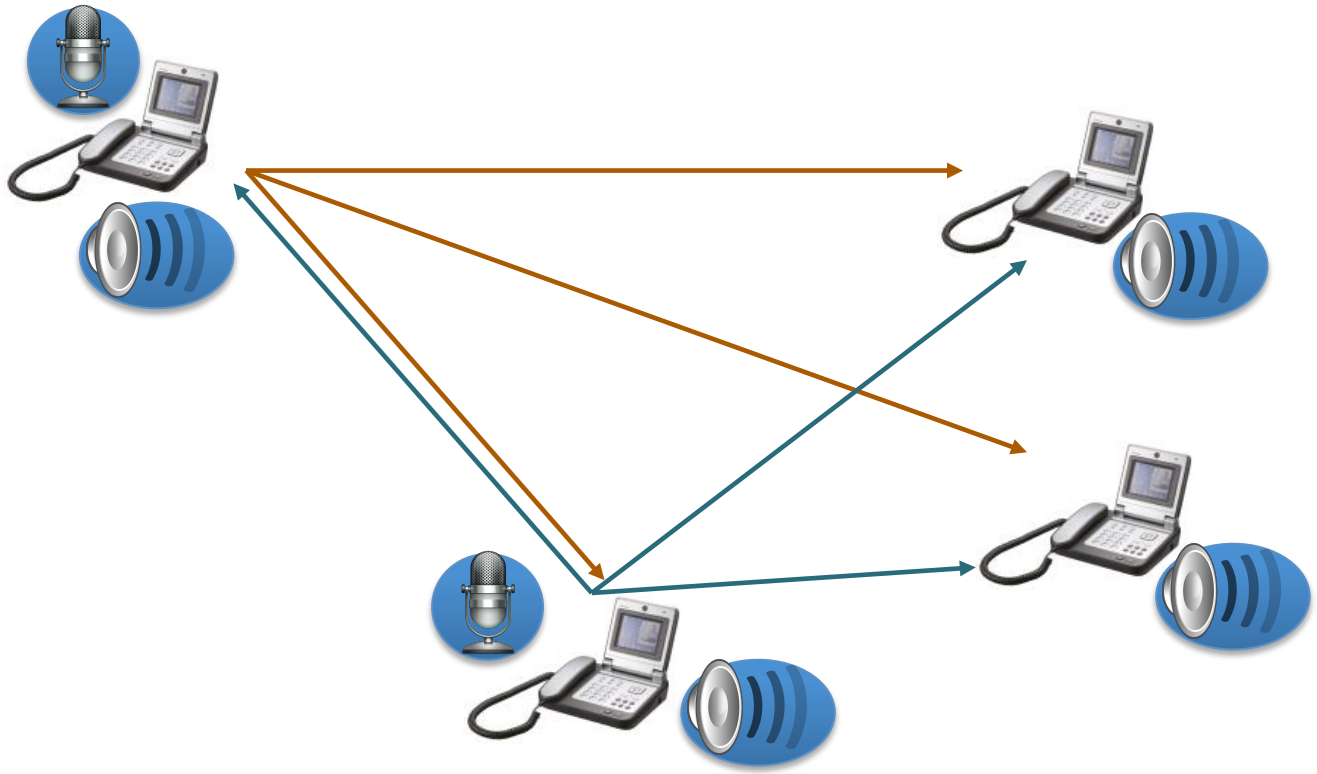
Unreliable Communication



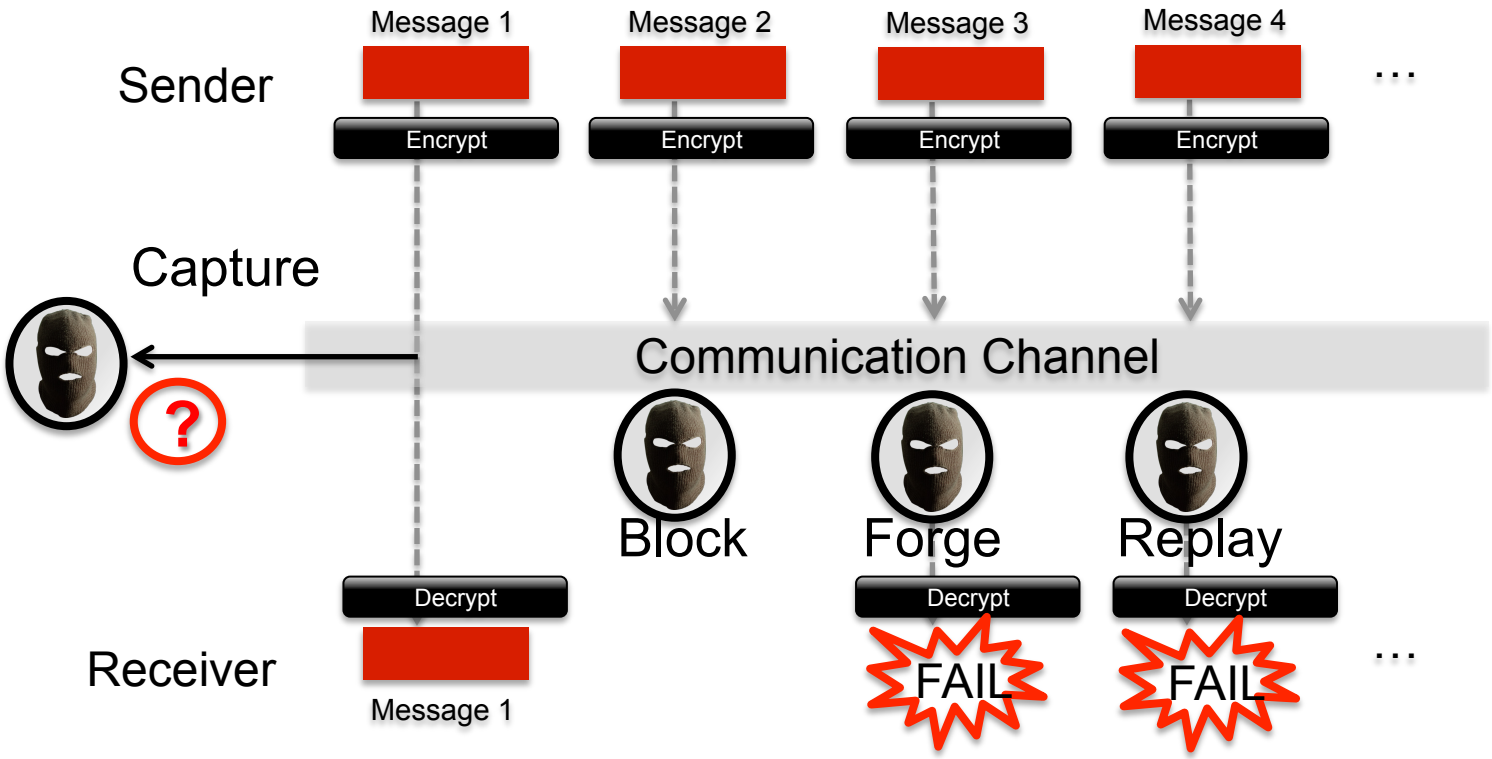
Multiple Receivers



Multiple Senders

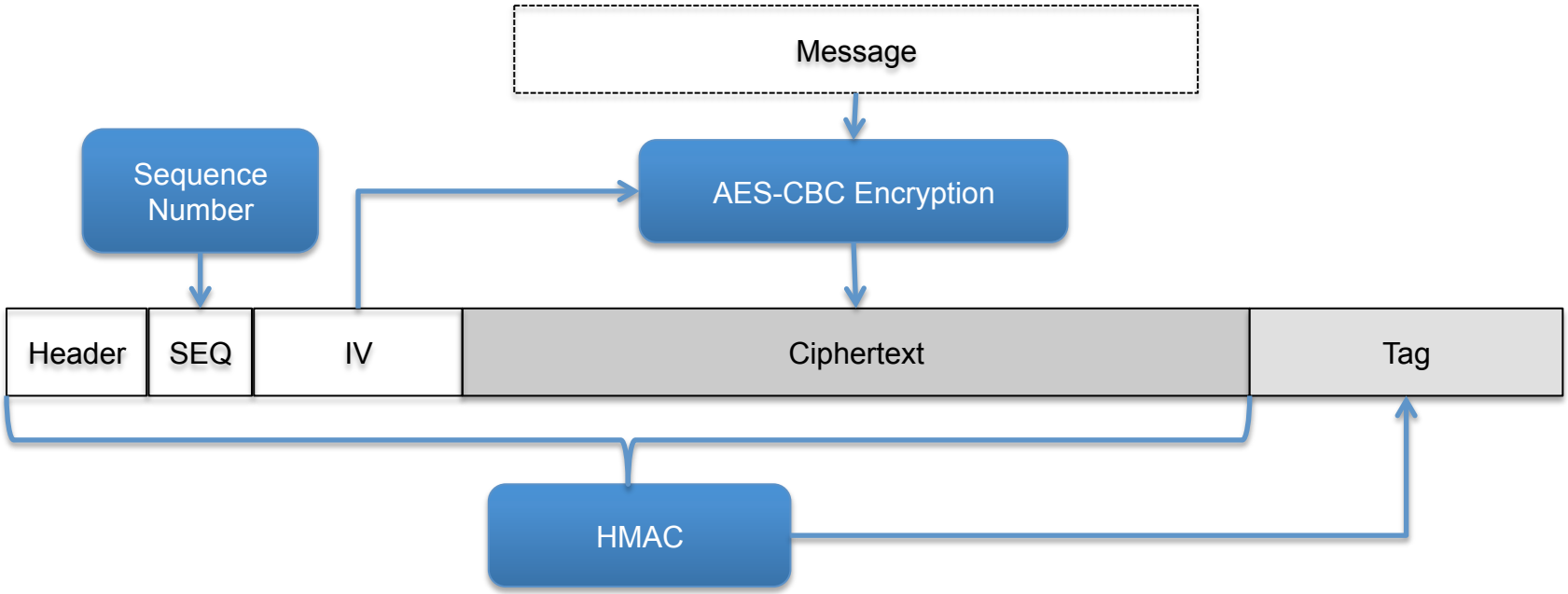


Authenticated encryption

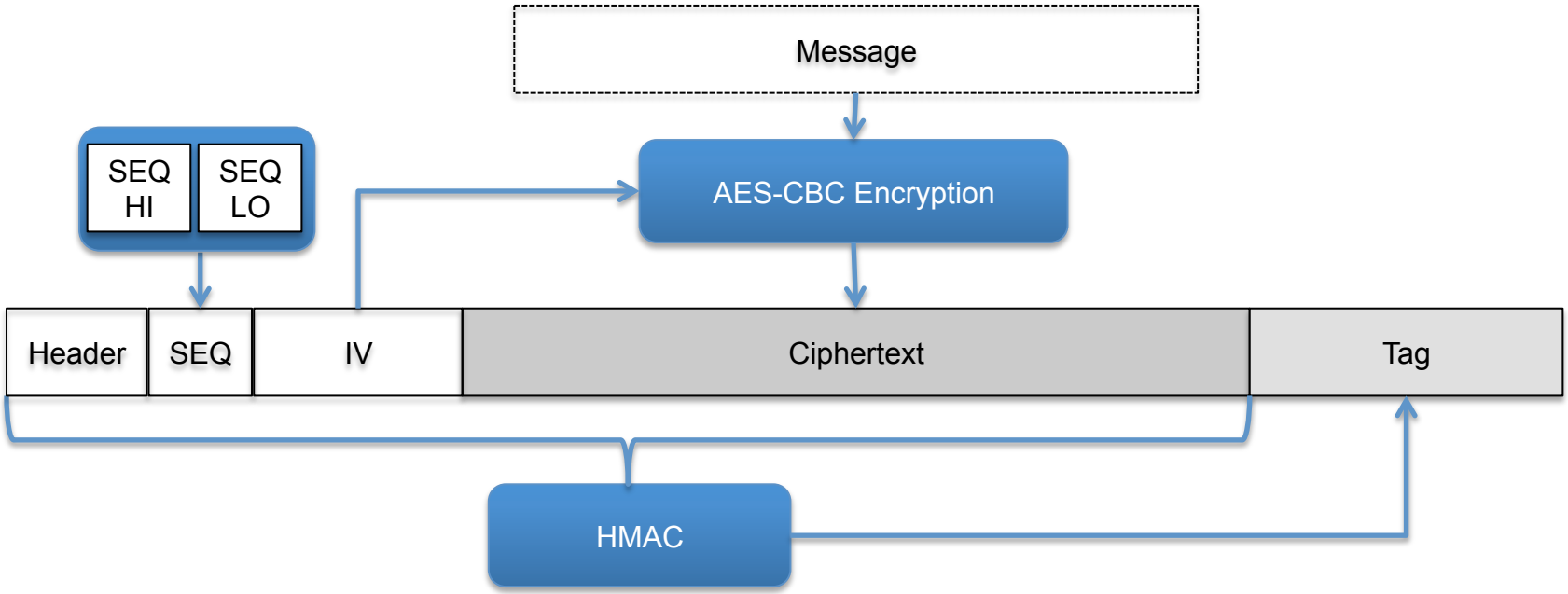


Conventional communication security

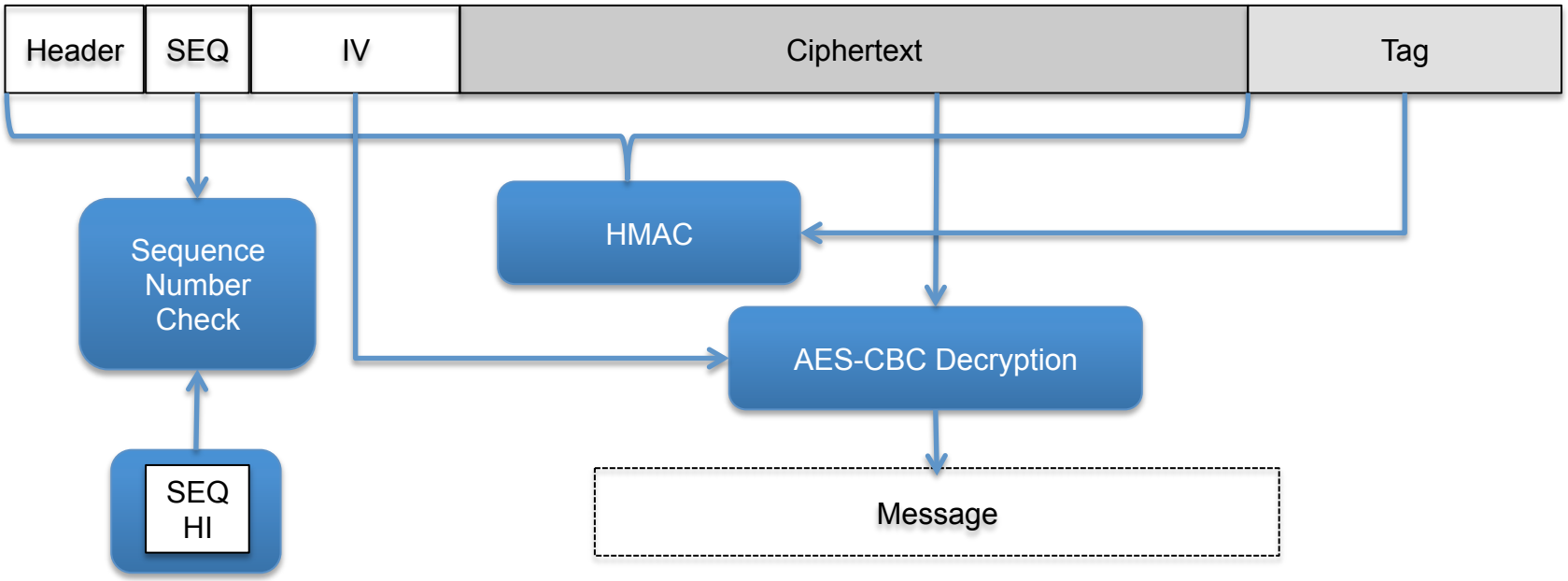
IPSec ESP


Message
Sequence Number
AES-CBC Encryption
Header
SEQ
IV
Ciphertext
Tag
HMAC

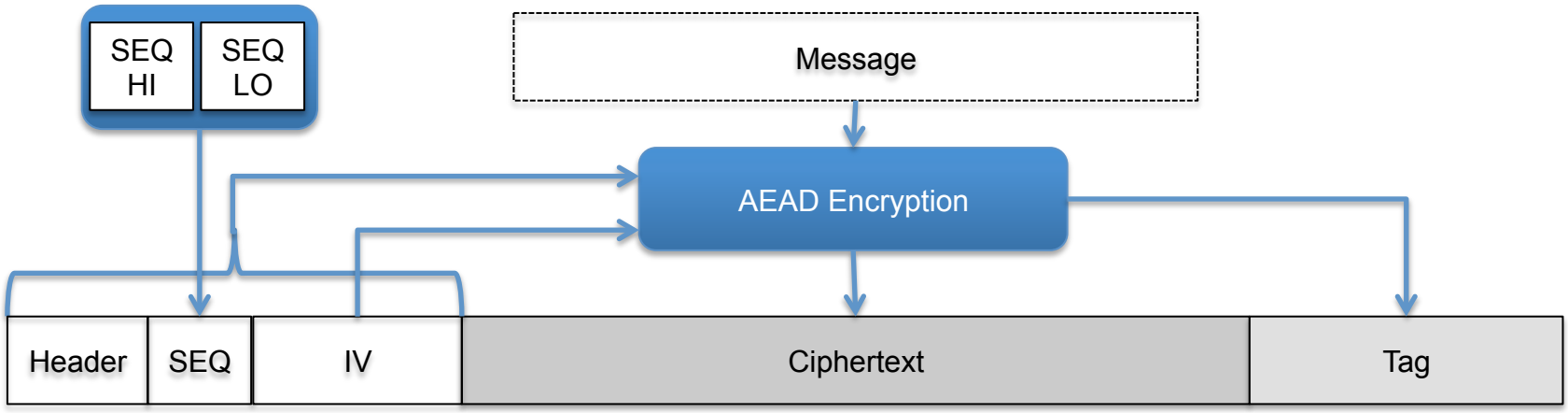
IPSec ESP


Message
SEQ HI
SEQ LO
AES-CBC Encryption
Header
SEQ
IV
Ciphertext
Tag
HMAC

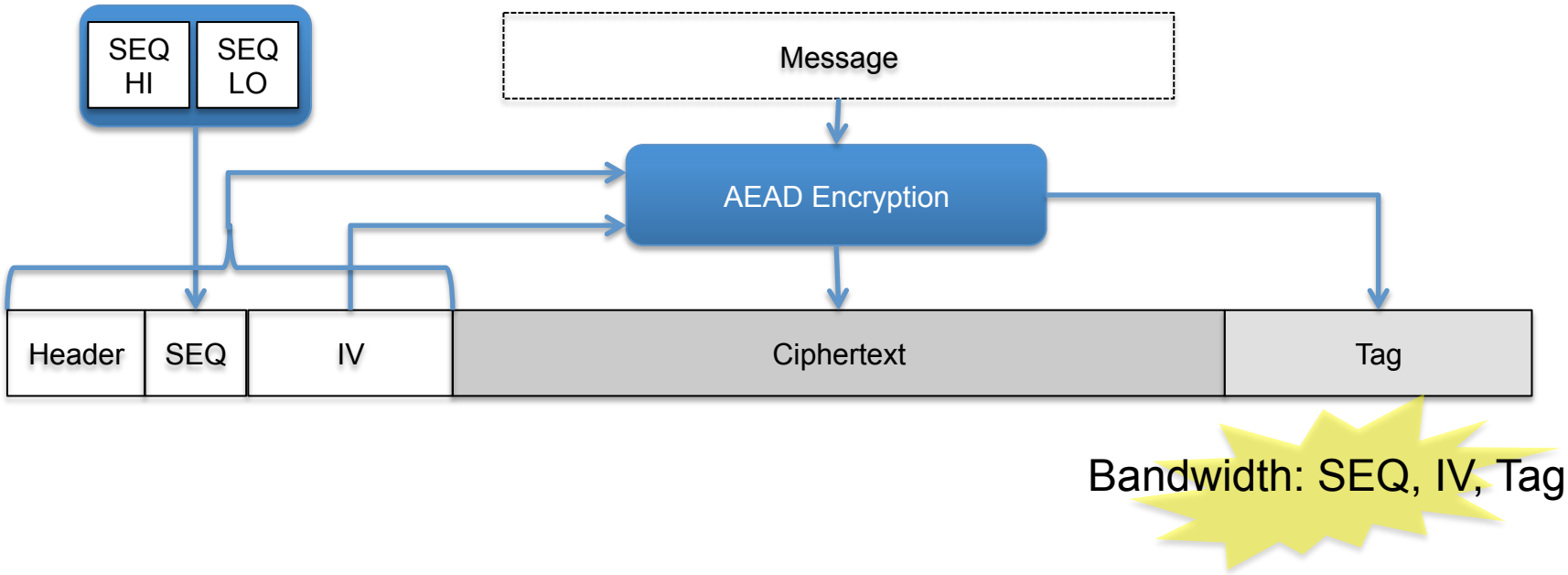
IPSec ESP


Header
SEQ
IV
Ciphertext
Tag
Sequence Number Check
HMAC
AES-CBC Decryption
SEQ HI
Message

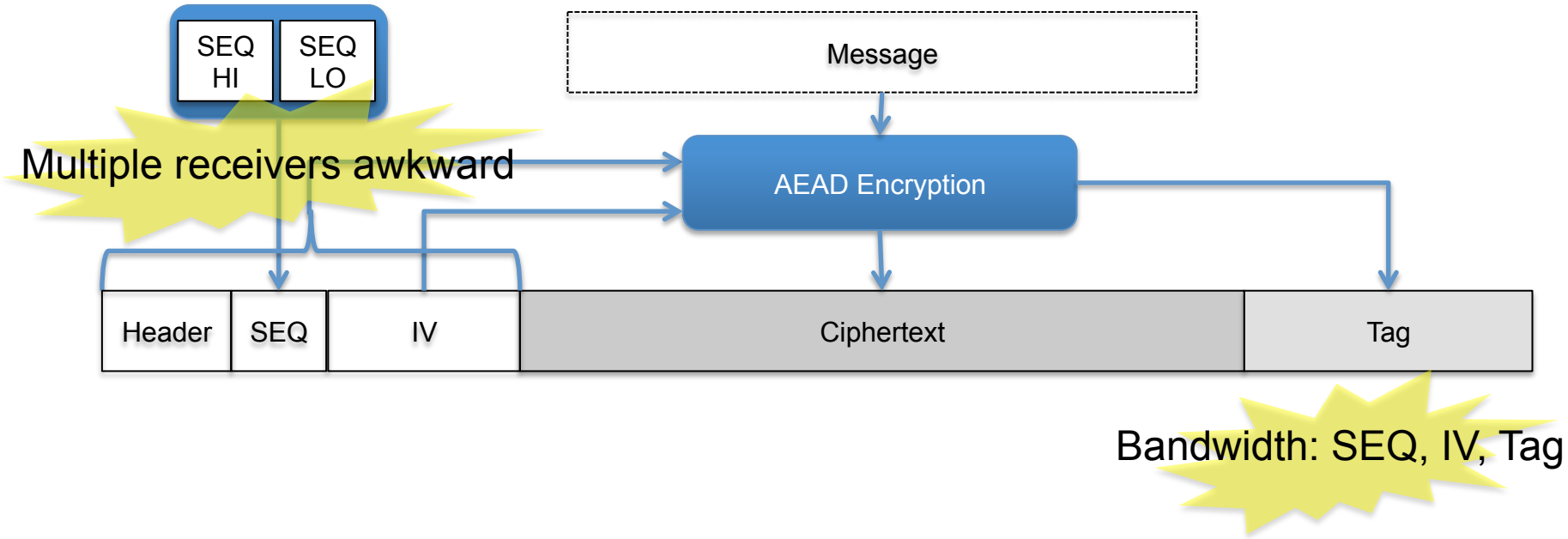
IPSec ESP with Authenticated Encryption



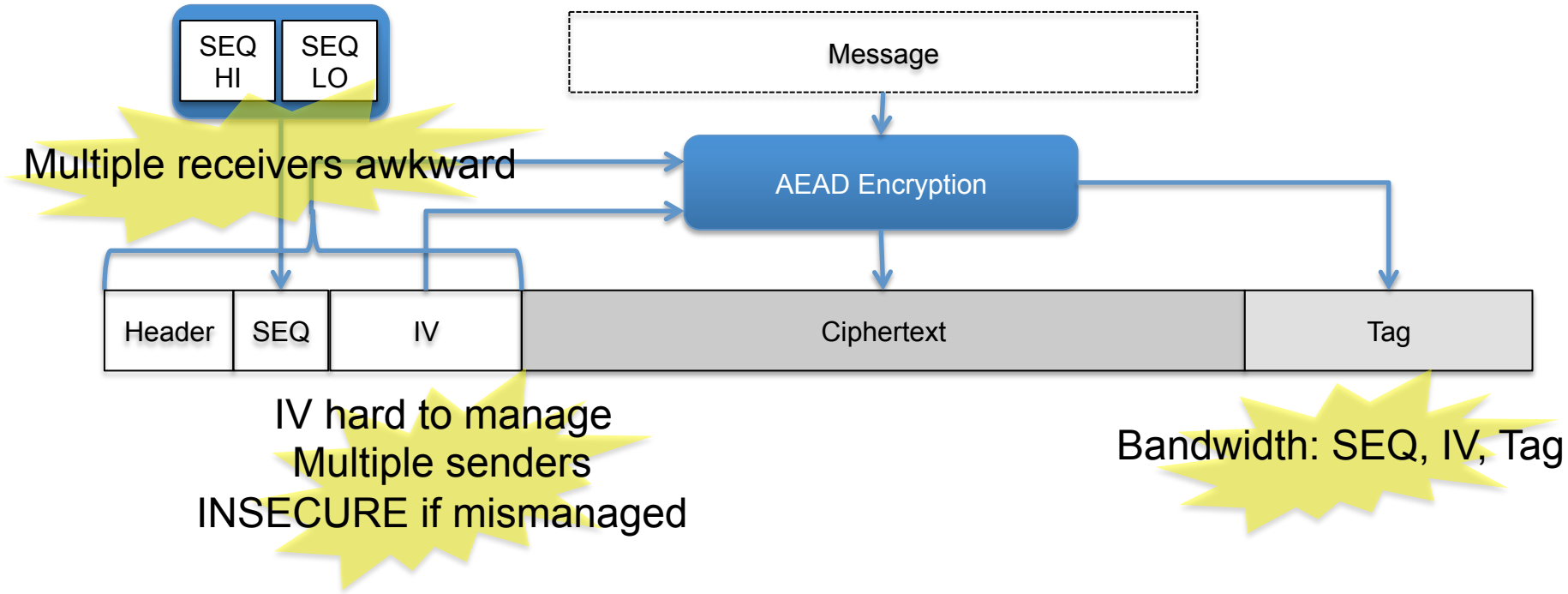
Problems with conventional practice



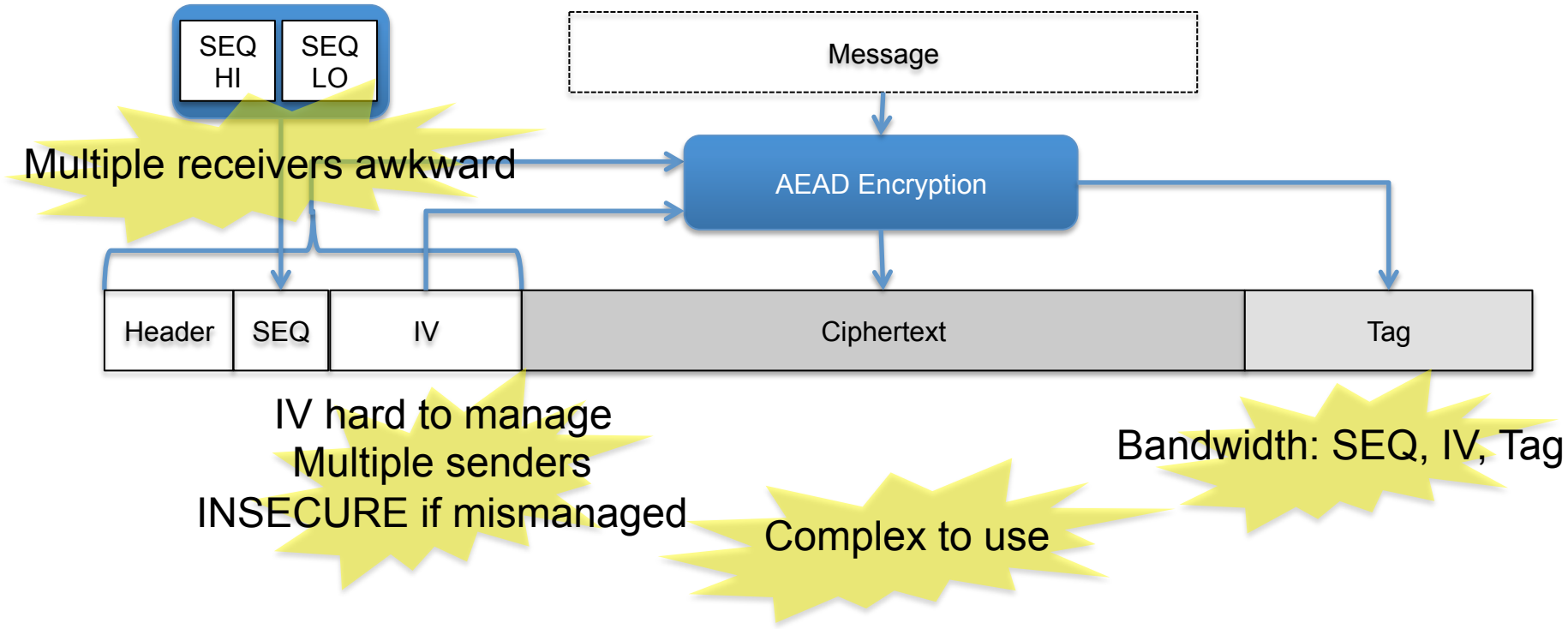
Problems with conventional practice



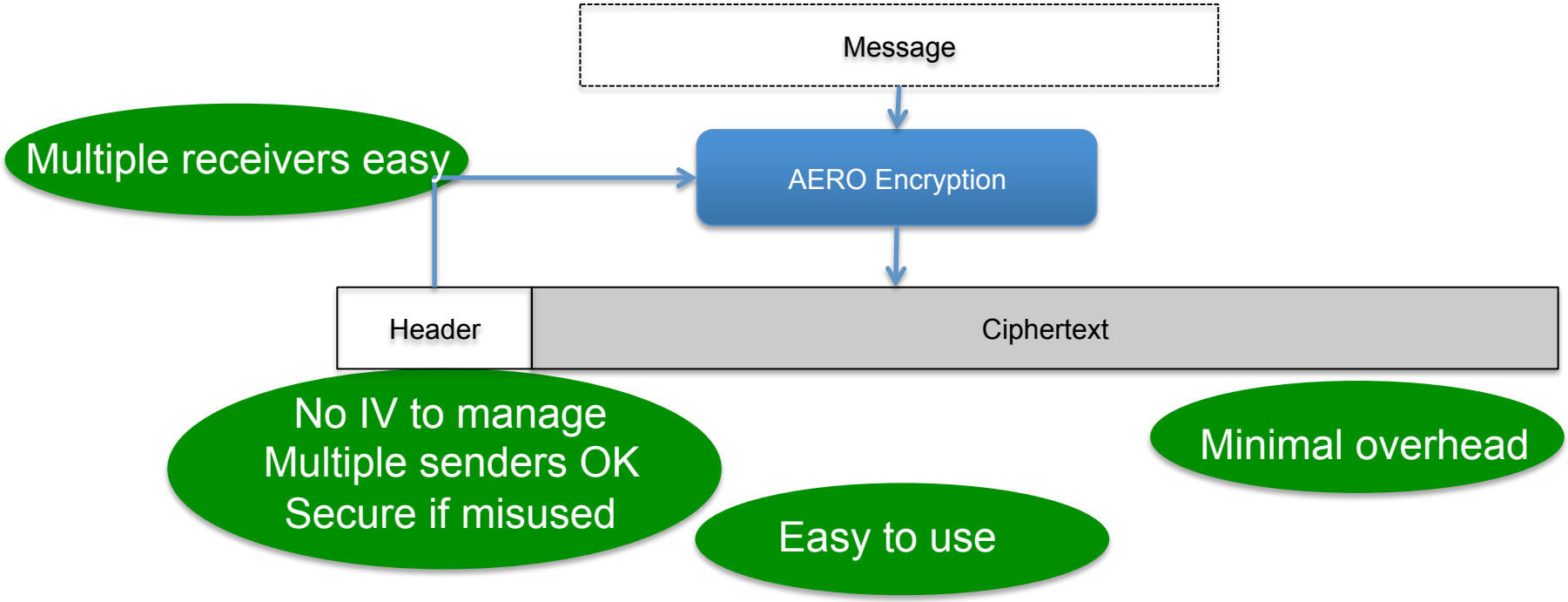
Problems with conventional practice



Problems with conventional practice



Authenticated Encryption with Replay prOtection

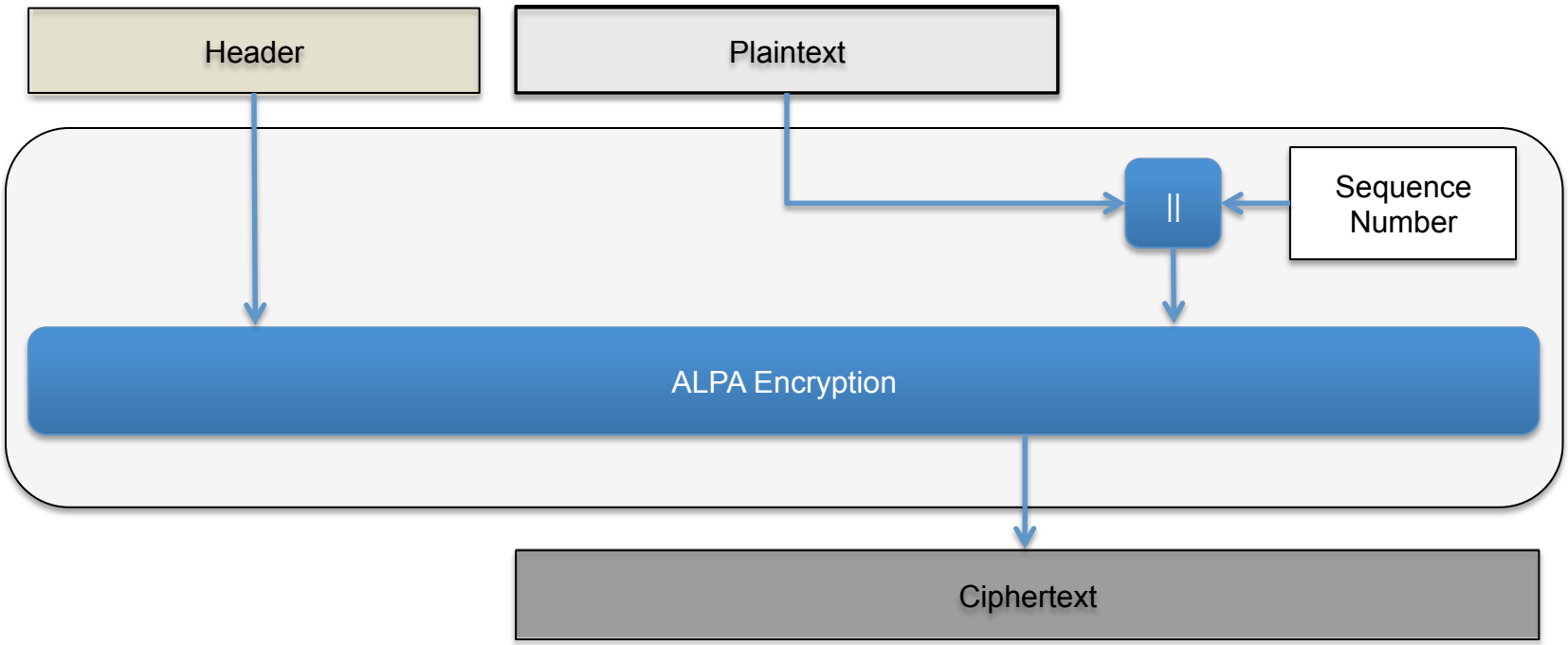


Authenticated Encryption with Replay prOtection (AERO)

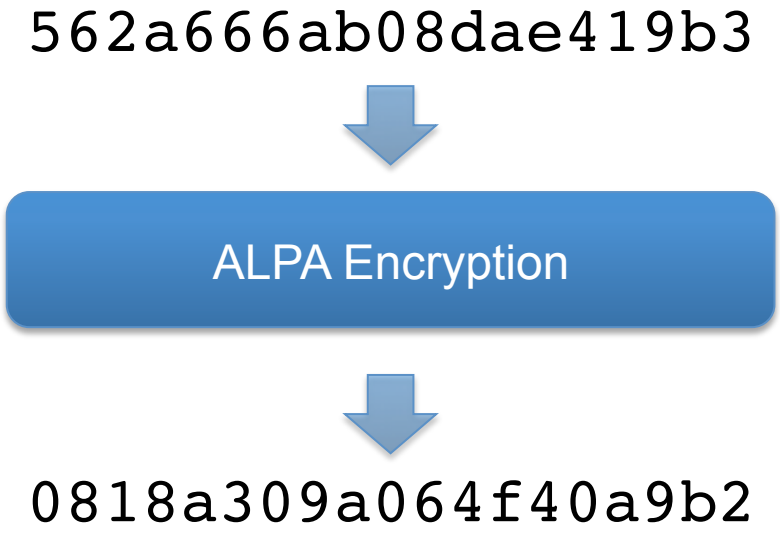
`draft-mcgrew-aero-01.txt`

Collaborators: John Foley, Stefan Lucks

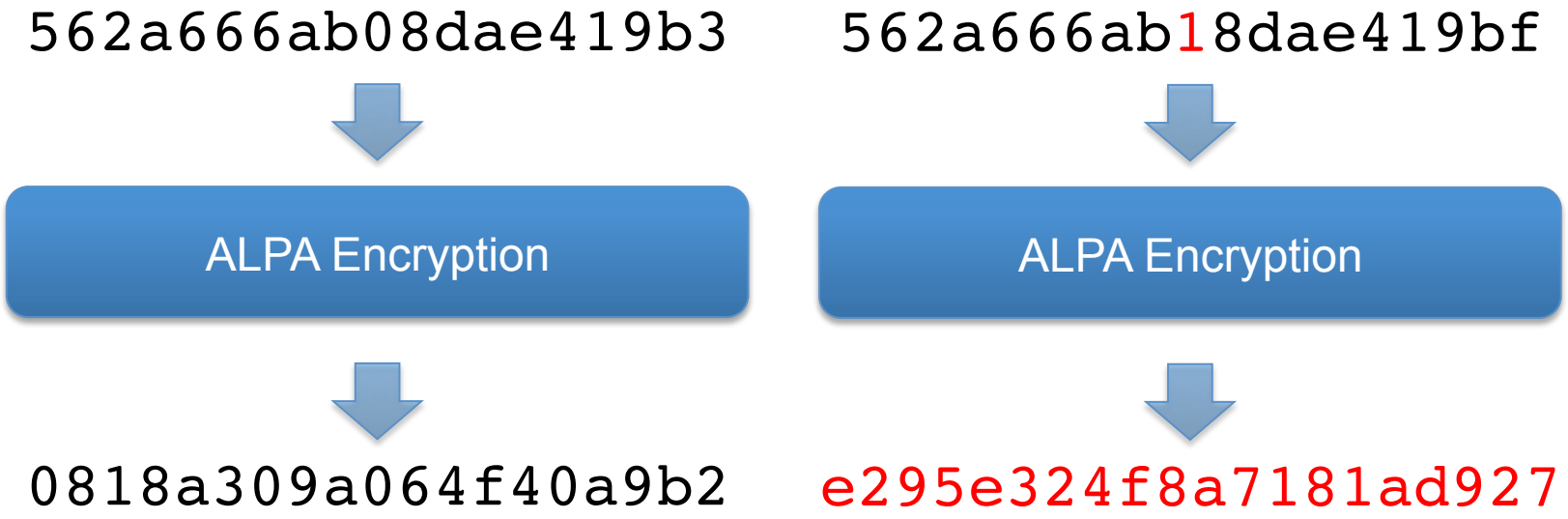
AERO Encryption



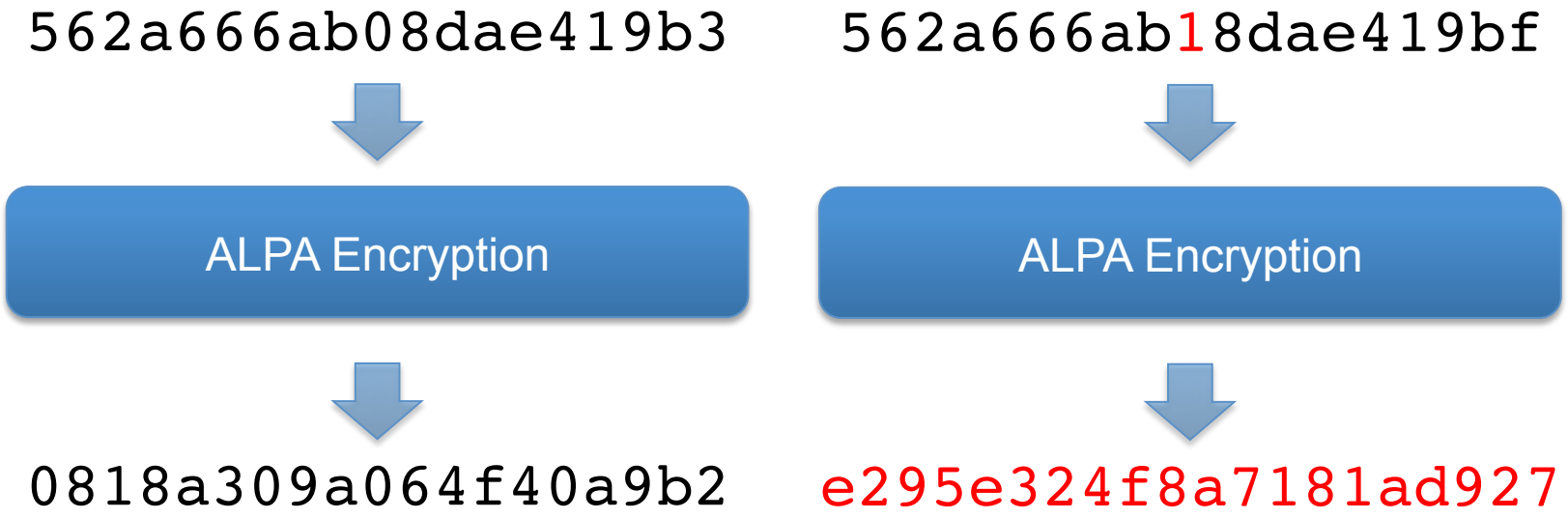
Arbitrary length permutation w/associated data



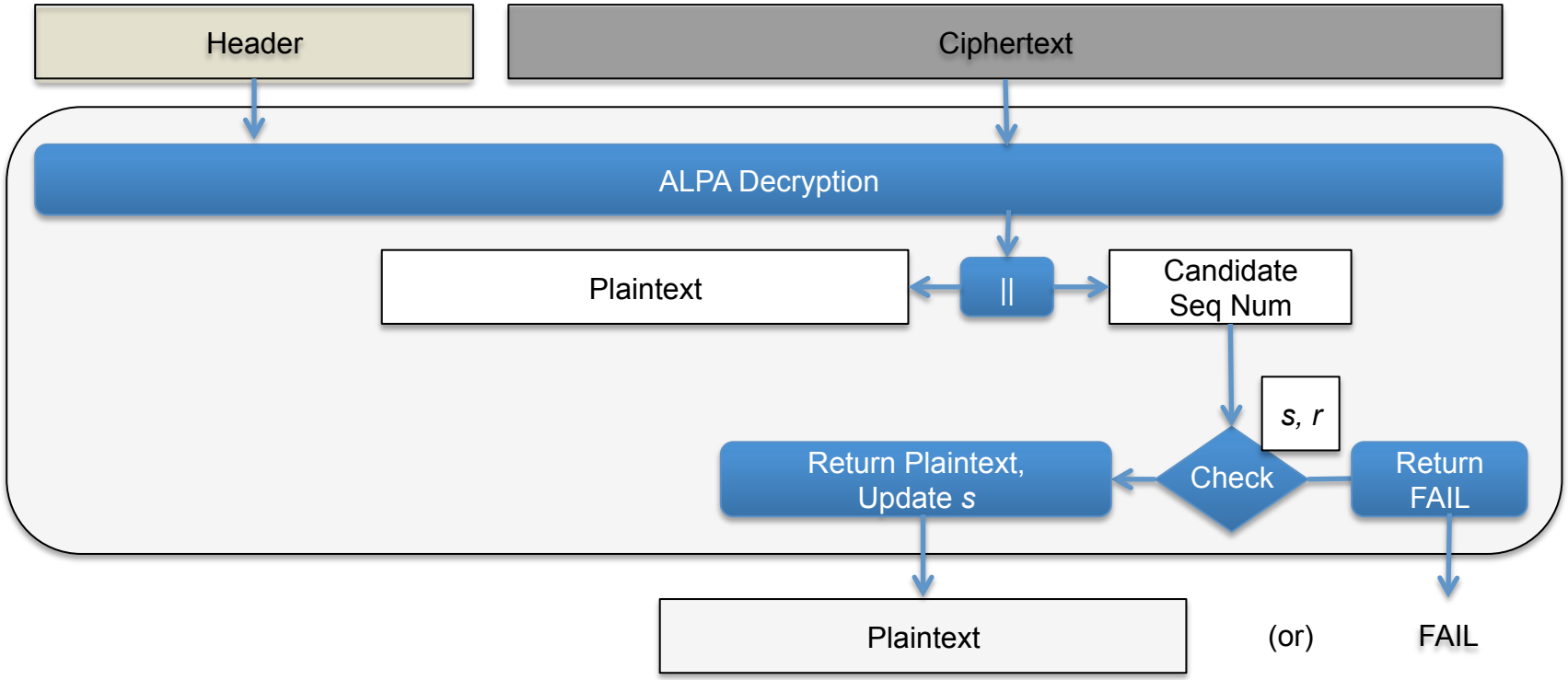
Arbitrary length permutation w/associated data



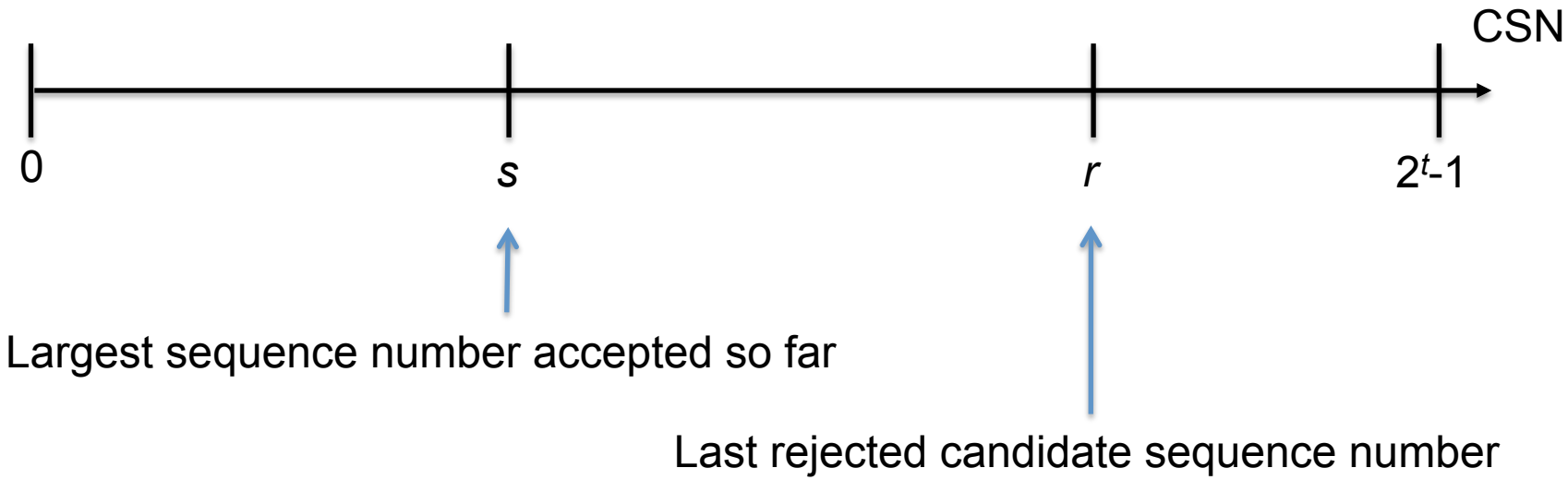
Arbitrary length permutation w/associated data



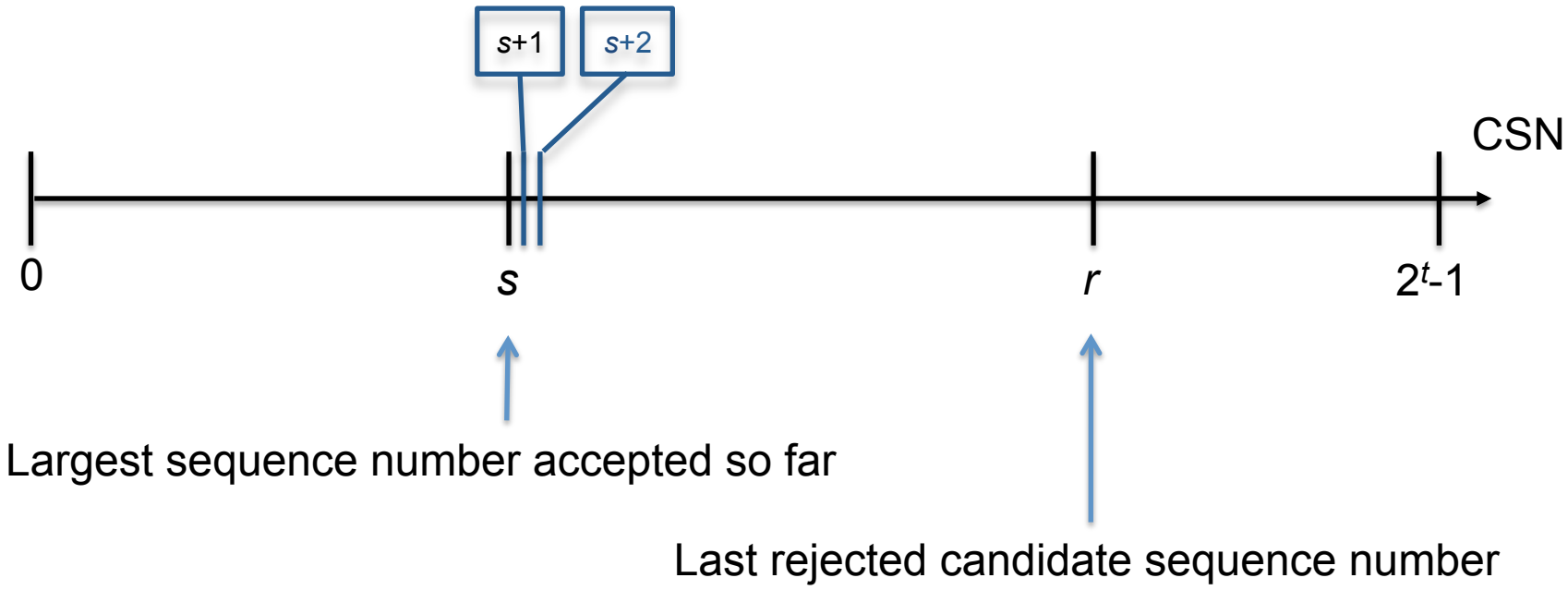
AERO Decryption



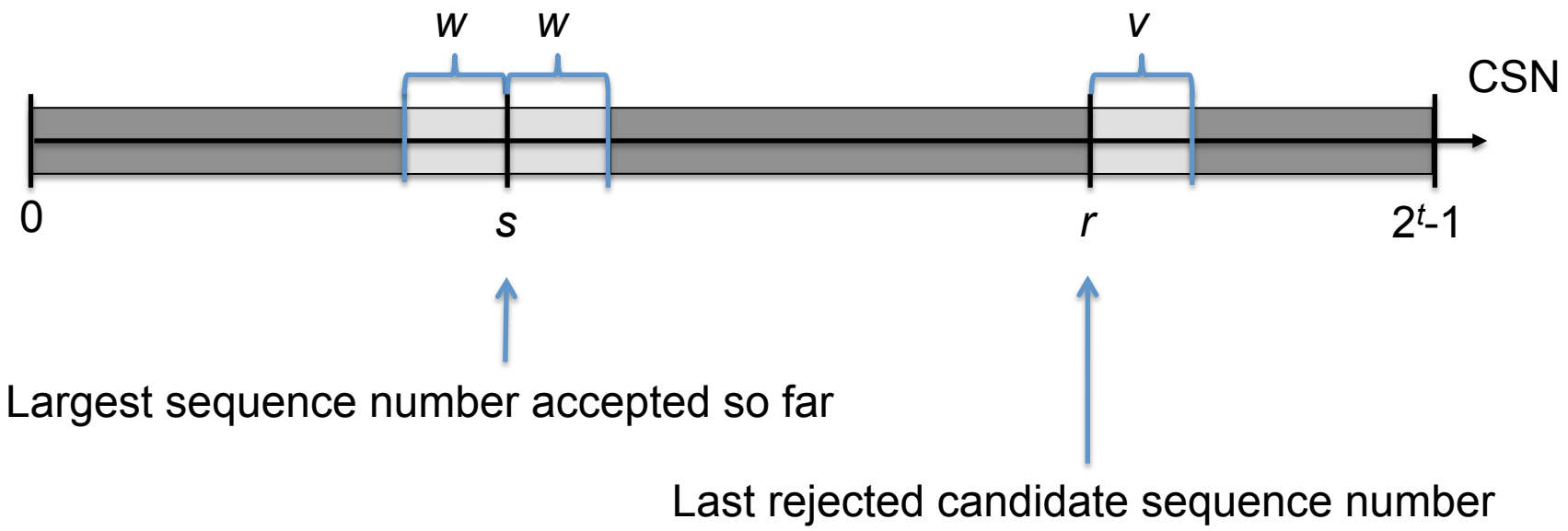
Candidate Sequence Number checking



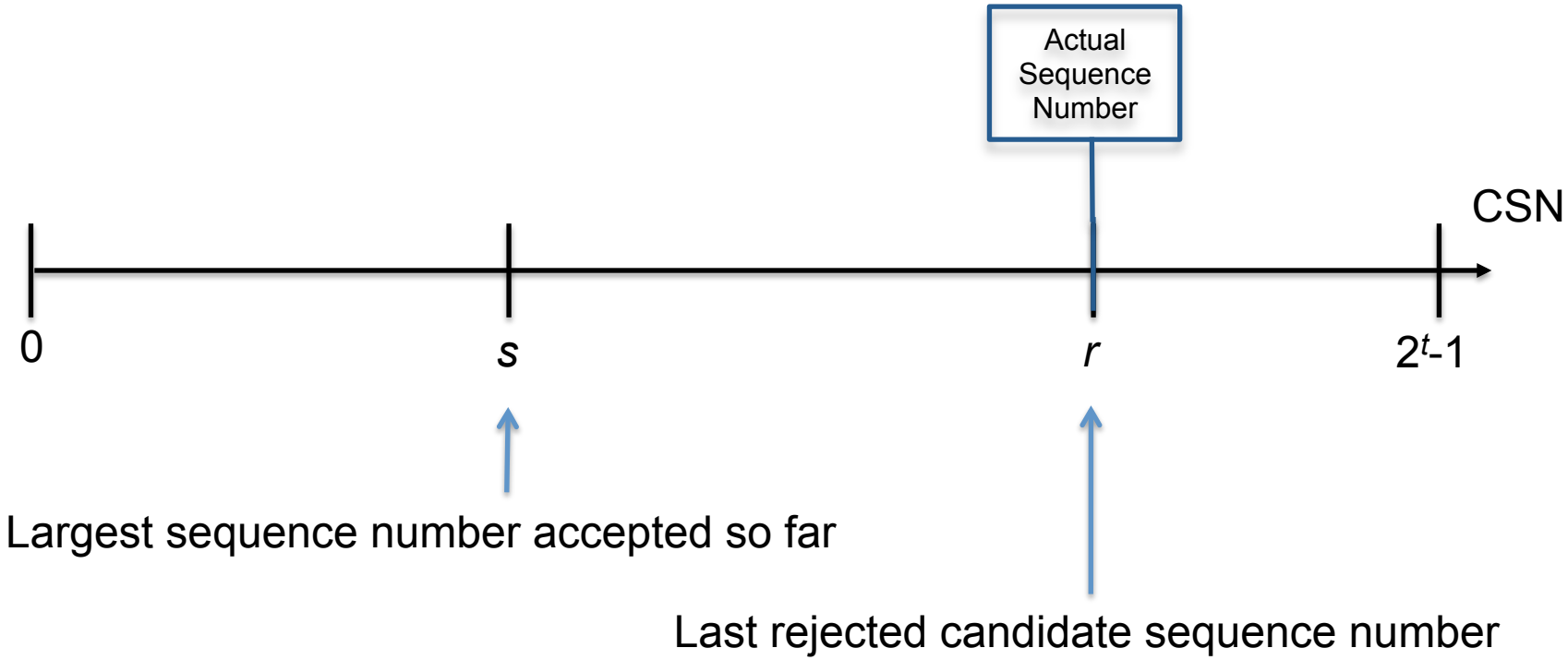
Likely next candidates



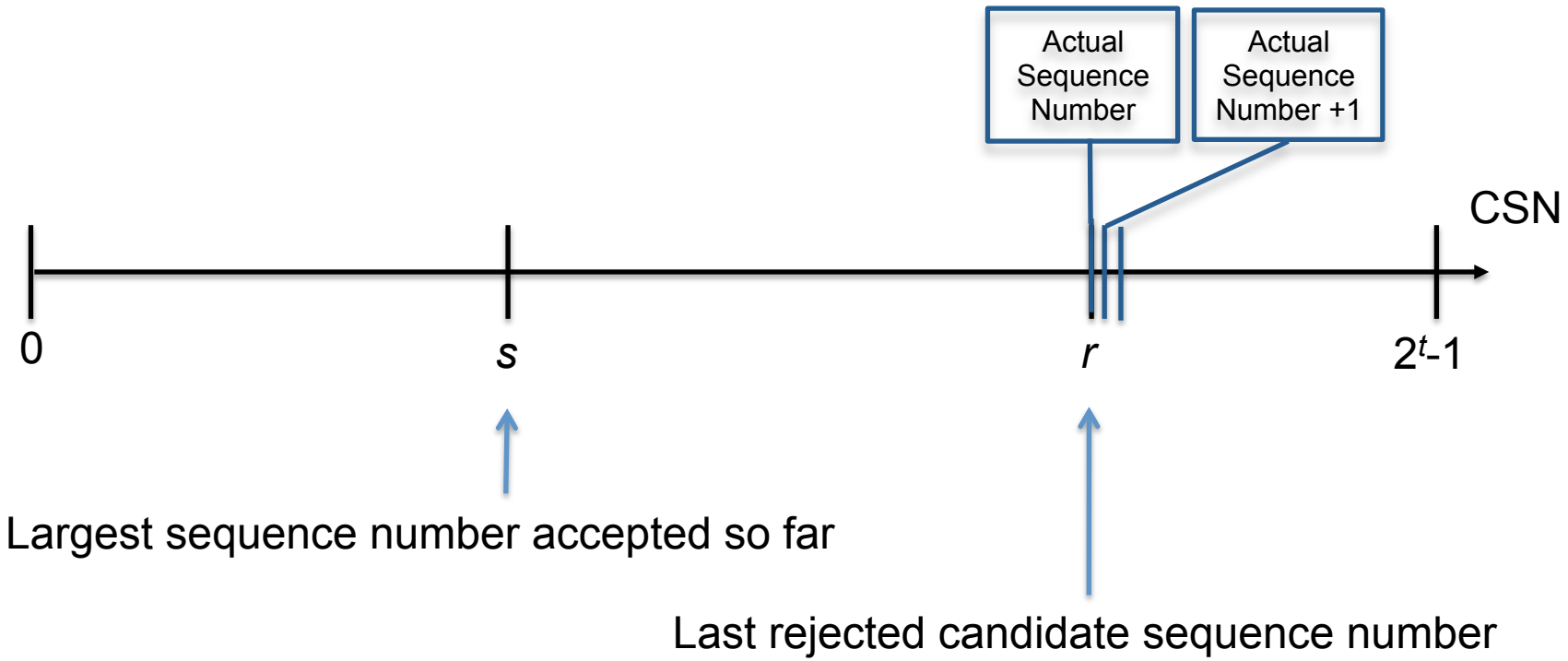
Candidate Sequence Number checking



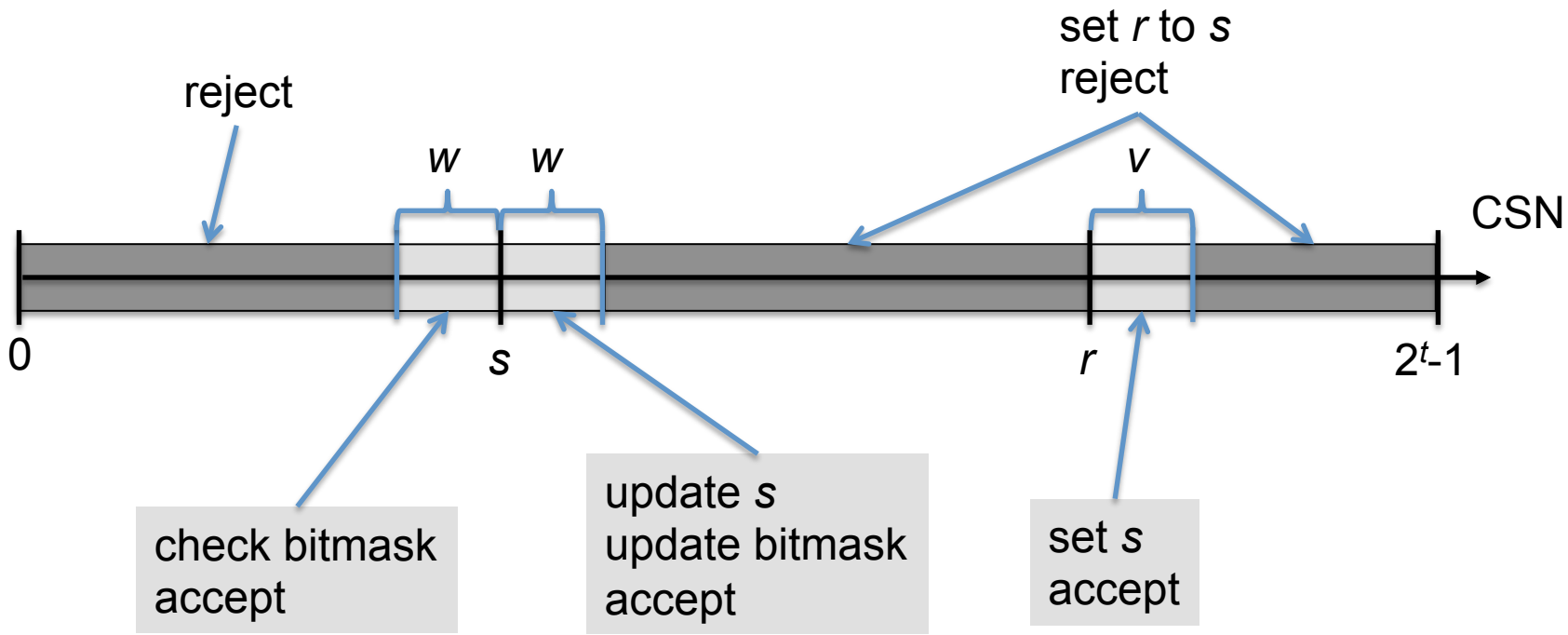
(Re)synchronization



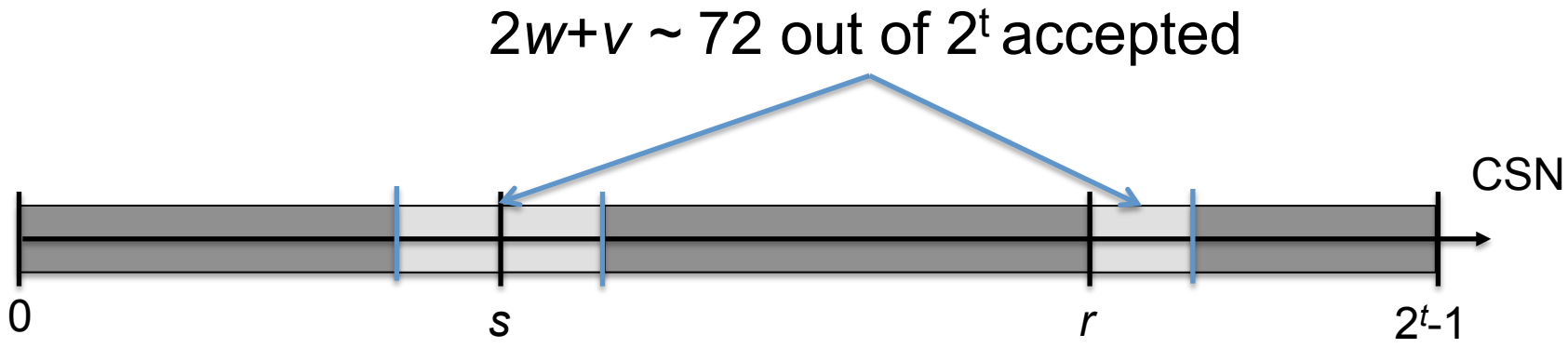
(Re)synchronization



Candidate Sequence Number checking



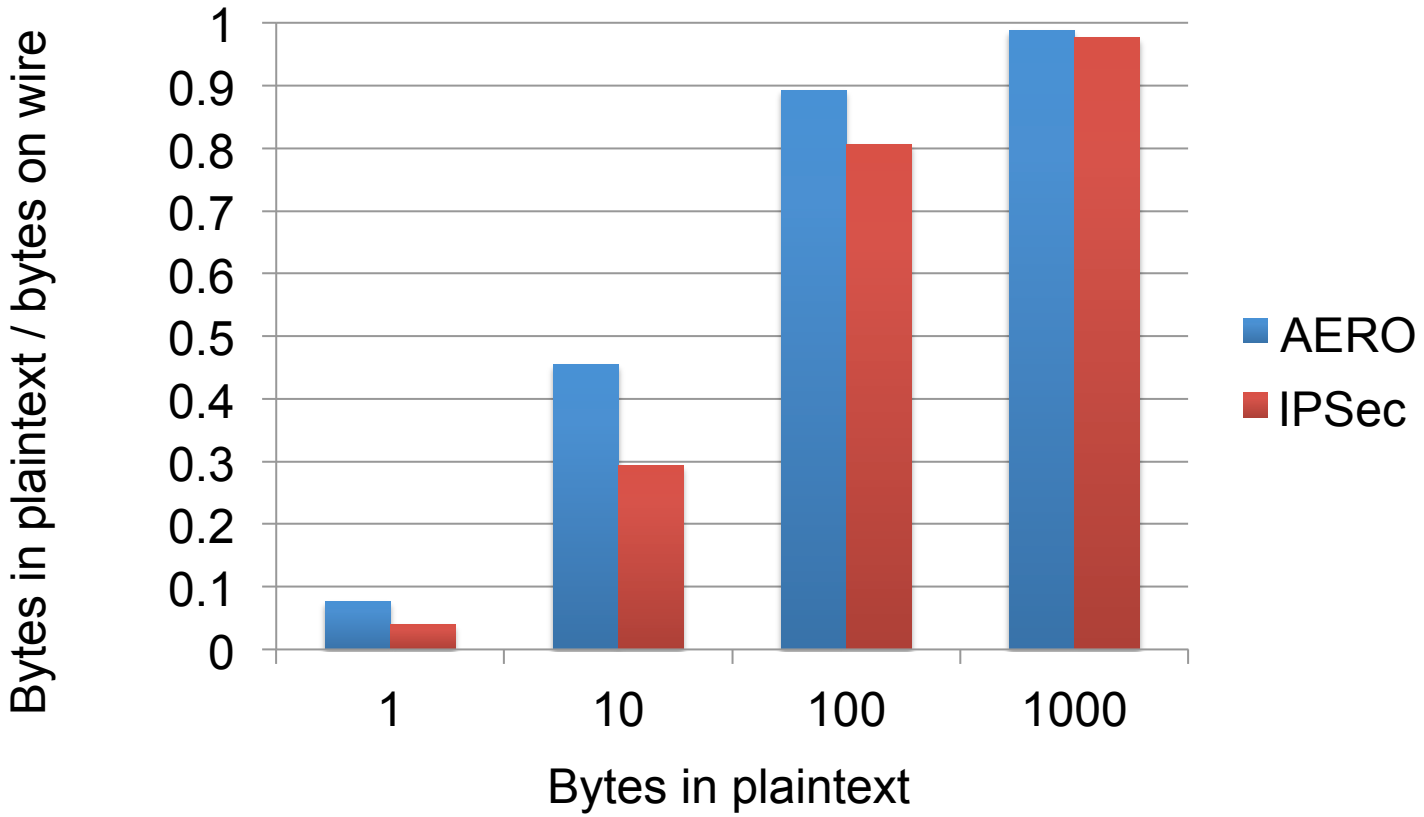
Security of authentication



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

AERO efficiency

Data efficiency



Primitives needed for AERO

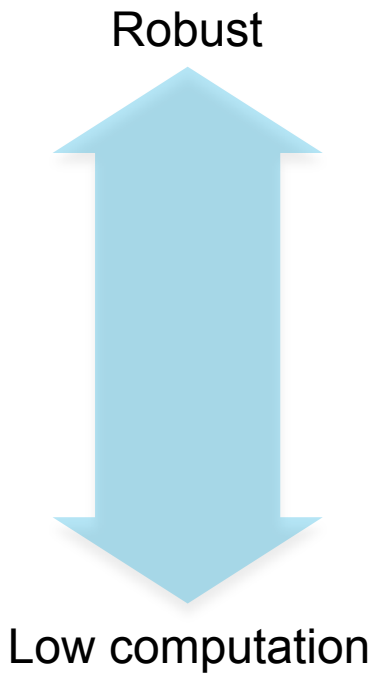
- Arbitrary length PRP

  Requires three (XCB) or four (LR) passes over data

- Online PRP

- AES-SIV adaptation (Stefan Lucks)

  IV = tweakable encryption of the sequence number, using the MAC as the tweak



XCB: IEEE 1619.2 *AES Extended Codebook Mode of Operation*

Conclusions

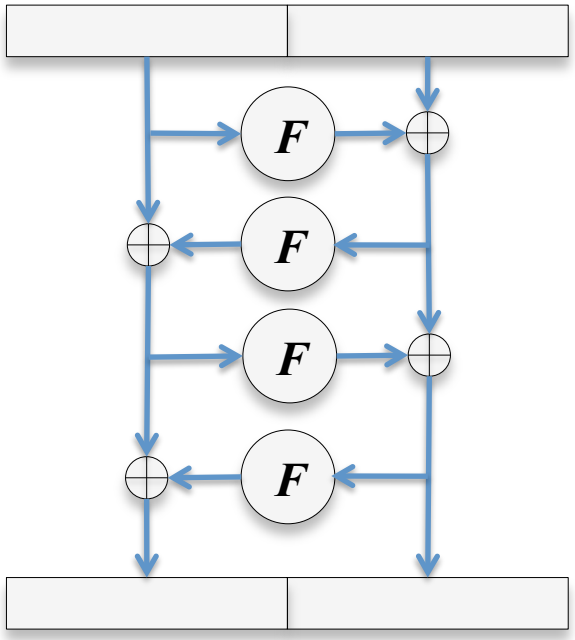
Conclusions

- Cryptography for low power wireless should
  - Minimize data overhead
  - Minimize computational cost
  - Be robust and simple
- Authenticated Encryption with Replay Protection
  - Can minimize data overhead
  - Analysis of primitives, performance, and security goals needed
- Opportunity

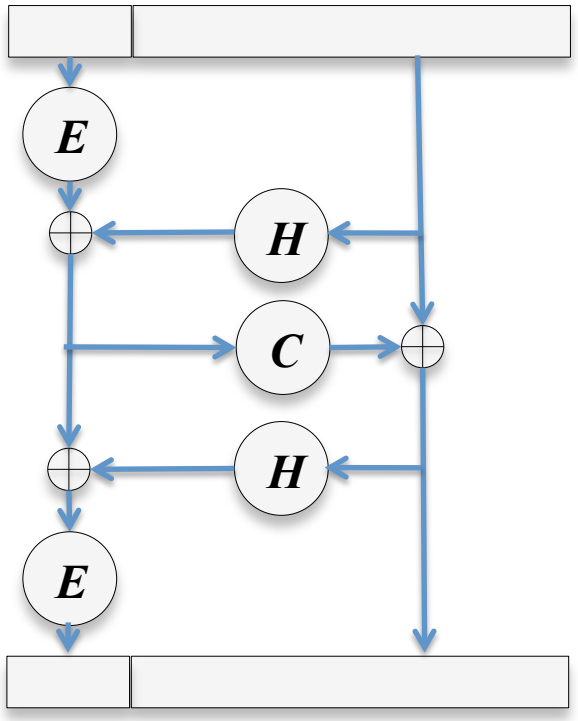
Thank you.

Backup slides

Arbitrary length PRP



Fiestel

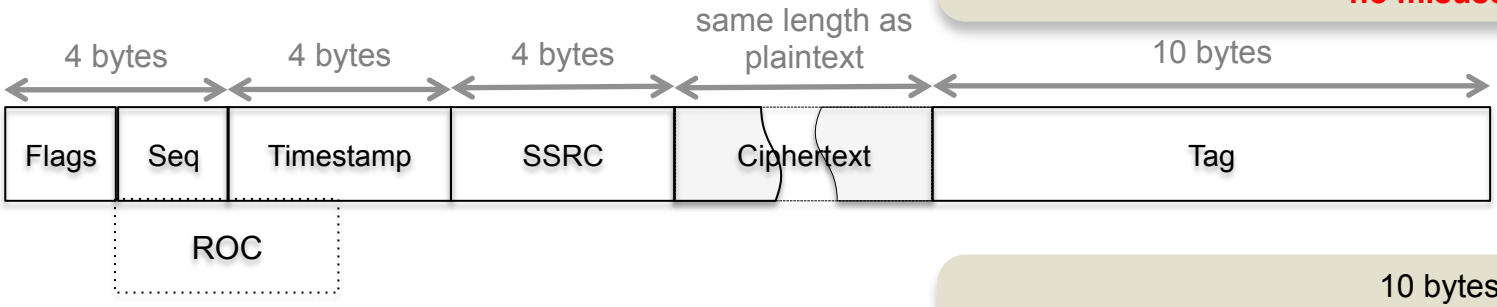


XCB

Secure RTP

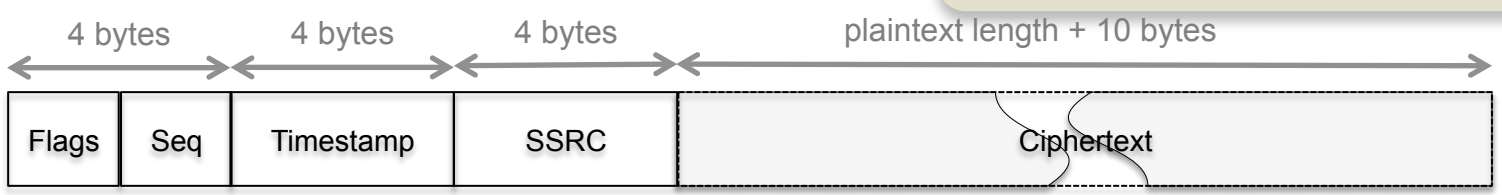
SRTP AES-CTR
HMAC-SHA1

10 bytes overhead per packet
4 bytes of state needing sync
no misuse resistance



SRTP AERO

10 bytes overhead per packet
no state needing sync
misuse resistance



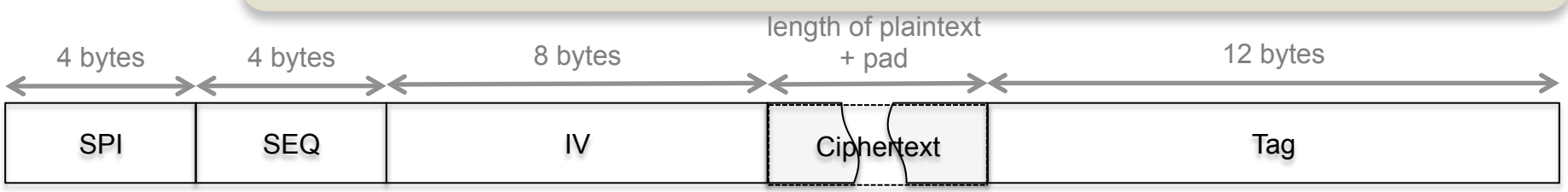
http://tools.ietf.org/search/draft-mcgrew-srtp-aero-01

IPSec

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

no misuse resistance

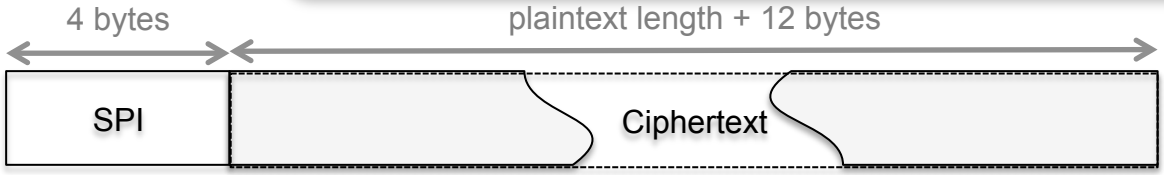
24+ bytes overhead per packet



ESP AERO

misuse resistance

12 bytes overhead per packet



AERO in Secure RTP

AERO in Secure RTP