InterMAClib: Beyond Confidentiality and Integrity in Practice

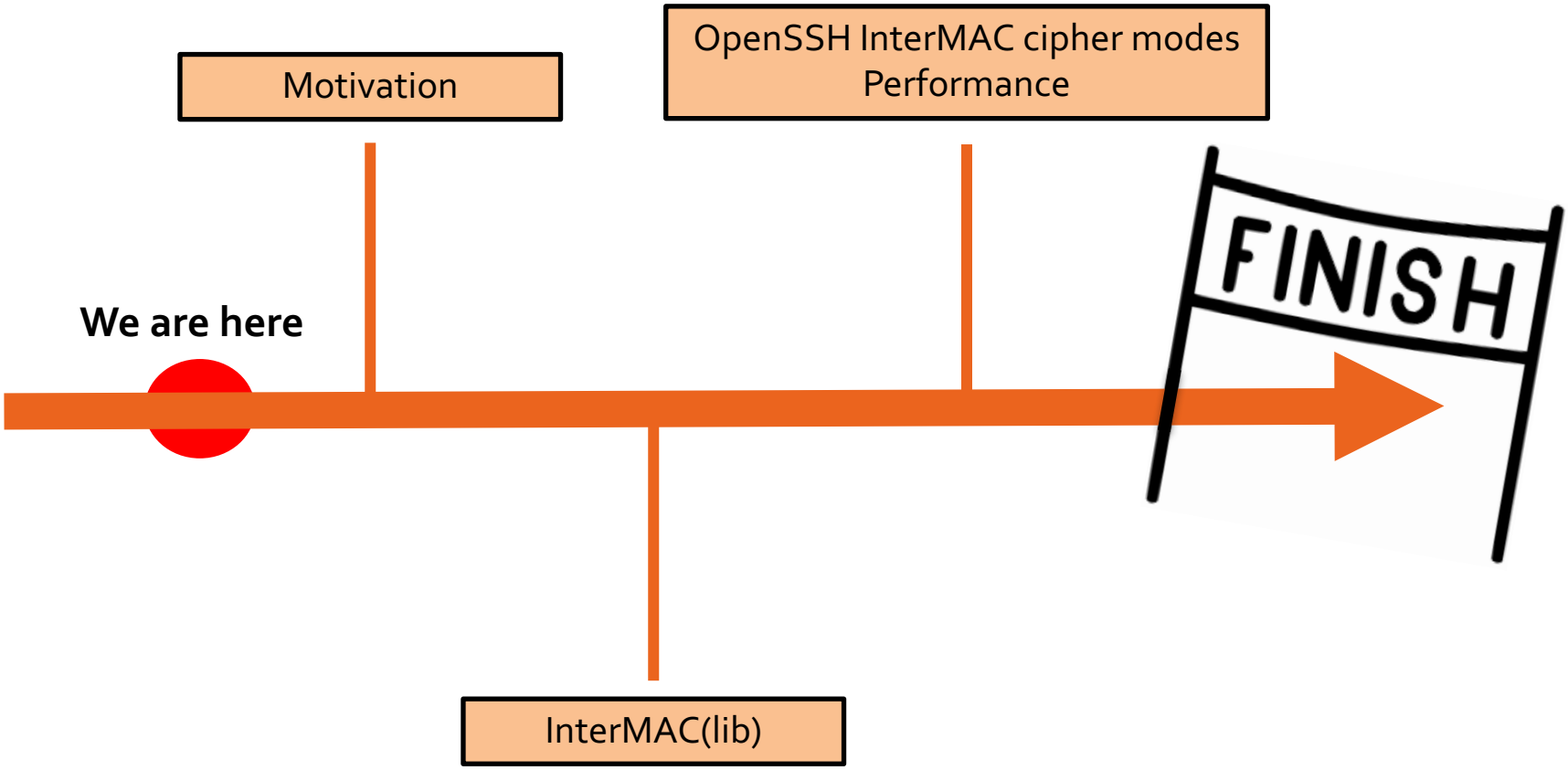
Torben B. Hansen @n_tbh
Joint work with
Martin R. Albrecht @martinralbrecht
Kenneth G. Paterson @kennyog

Information Security Group
Centre for Doctoral Training in Cyber Security

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Real World Crypto 2018 January 12th

The next ~25 mins

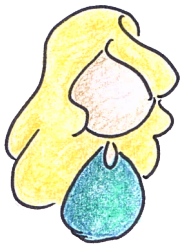


Symmetric encryption

Modelling security

AE

$C \leftarrow Enc_k(M)$



C

$M \leftarrow Dec_k(C)$

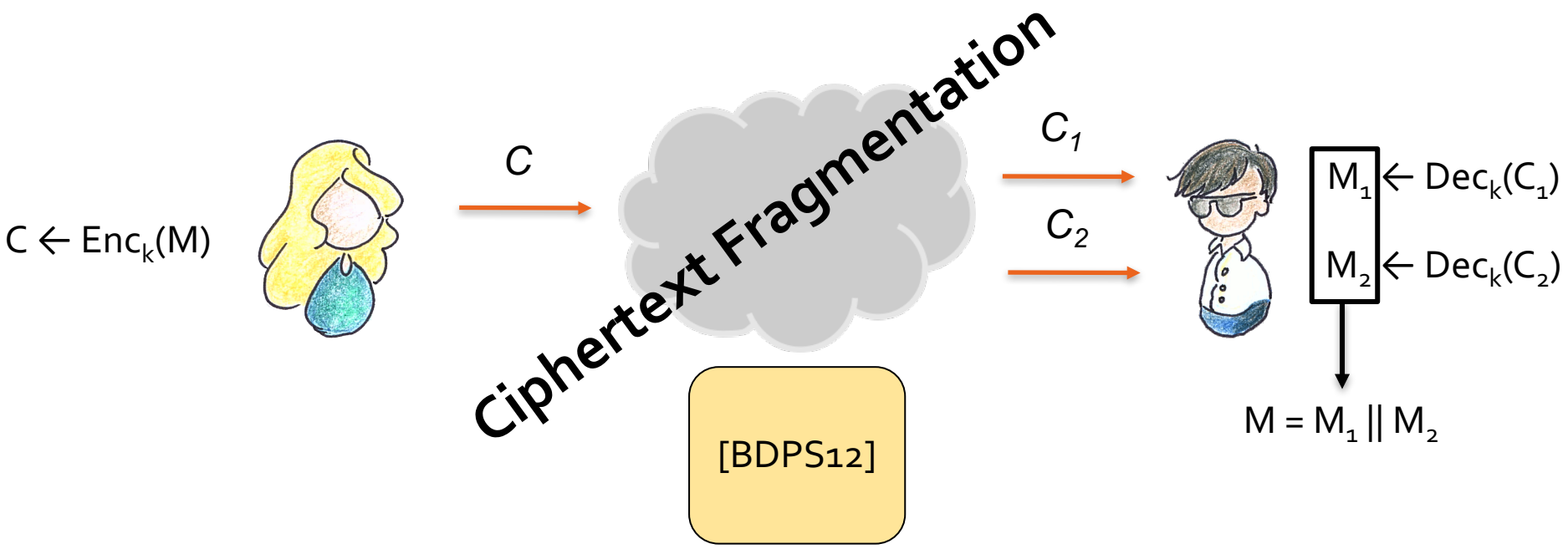
Good approximation?

[BKN02]

SSH CBC-mode is secure!

[APW09]

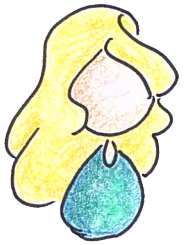
SSH CBC-mode is **not** secure!



SSH packets contains a length field

Security notions

$C \leftarrow Enc_k(M)$



C

C_1

C_2

$M_1 \leftarrow Dec_k(C_1)$

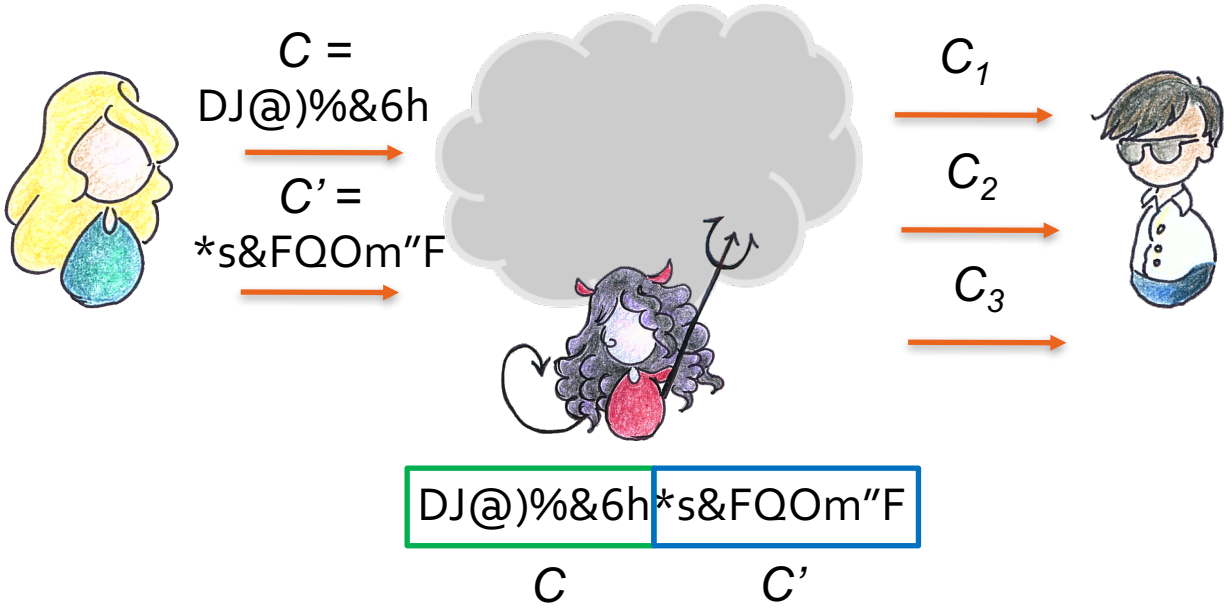
$M_2 \leftarrow Dec_k(C_2)$

$M = M_1 \,||\, M_2$

~~IND-CCA~~ → IND-sfCFA

~~IND-CTXT~~ → IND-sfCTF

Security notions



~~IND-CCA~~ → IND-sfCFA

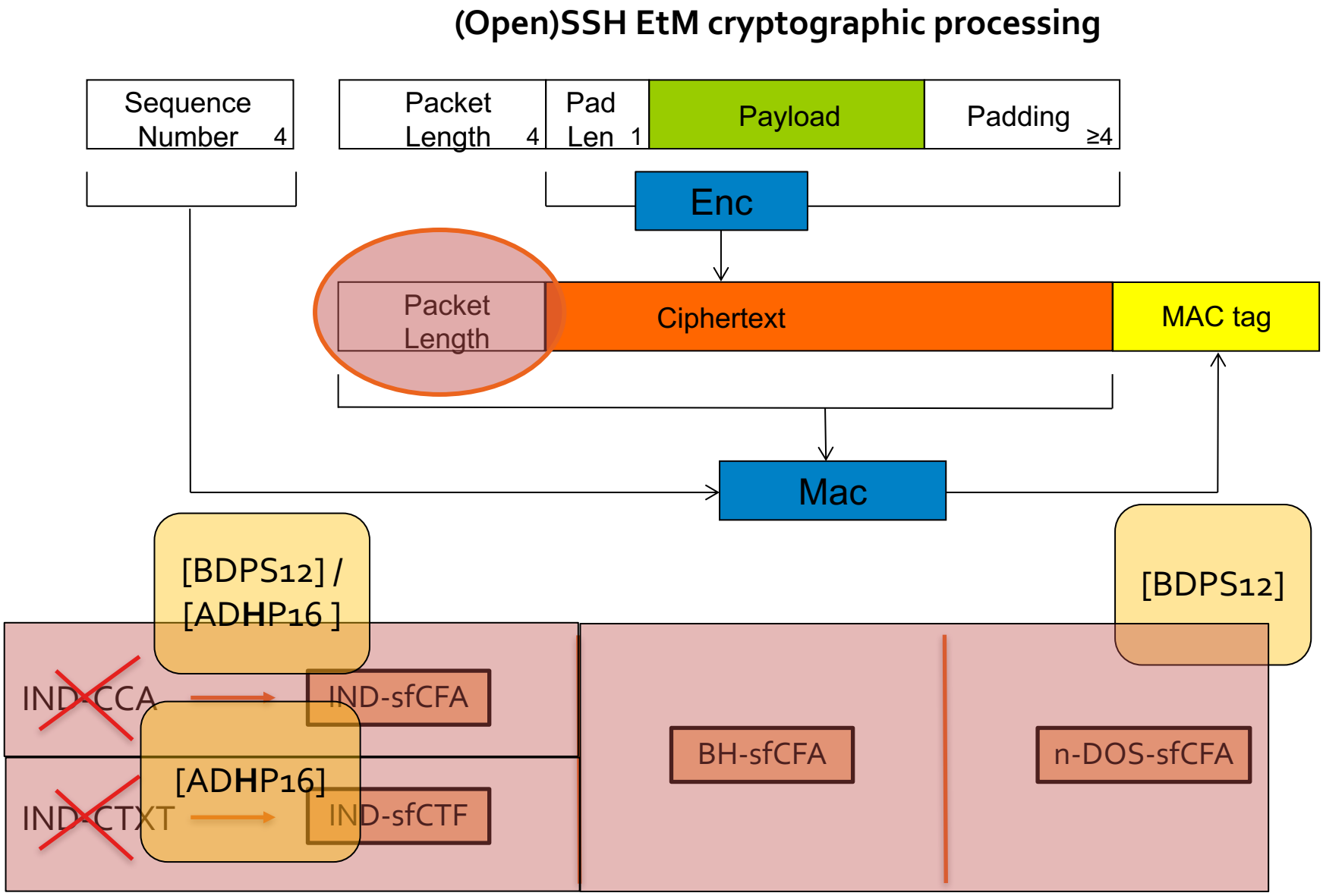
~~IND-CTXT~~ → IND-sfCTF

BH-sfCFA

SSH:

- Length field encrypted
- Random amount of padding

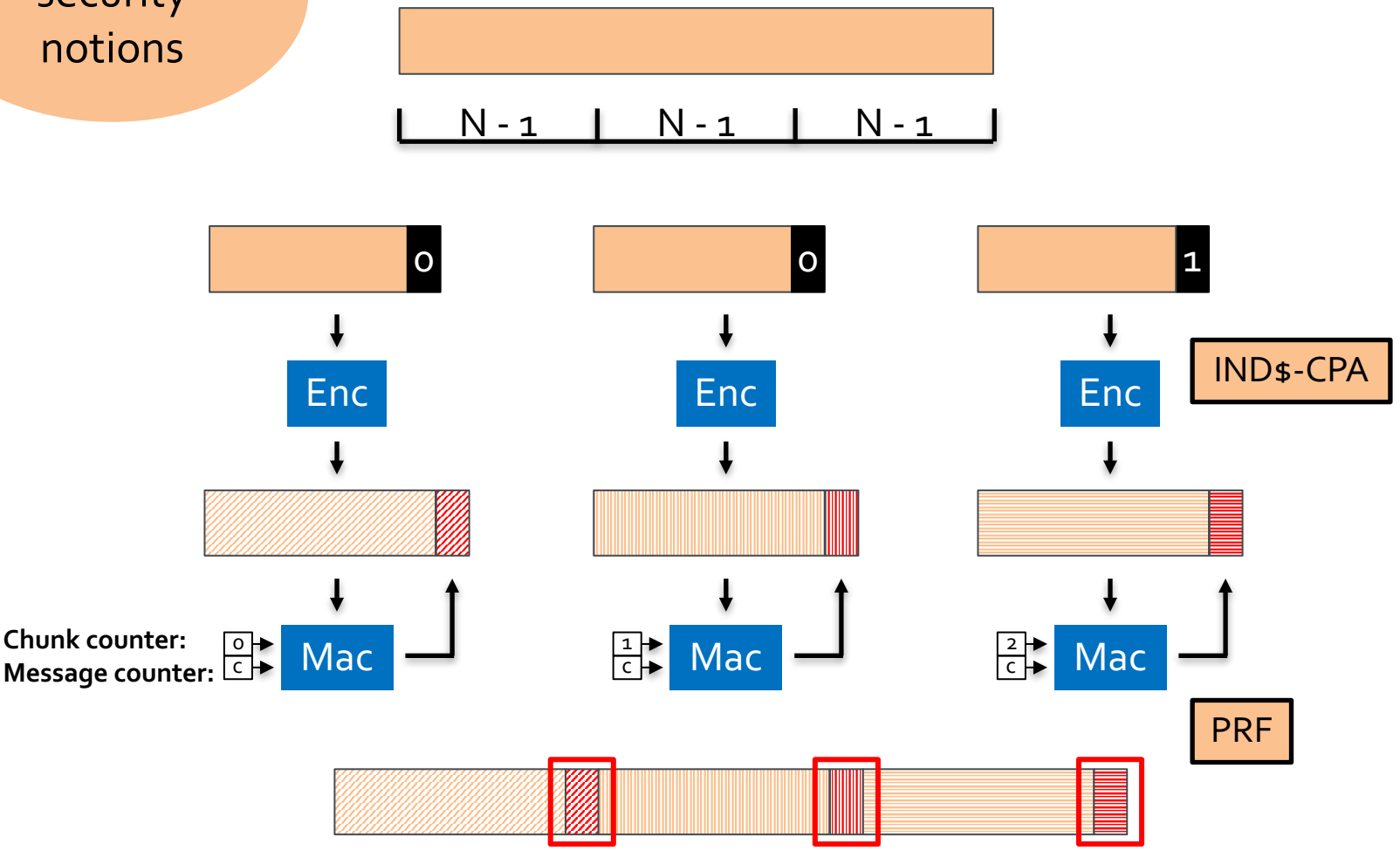
Security notions



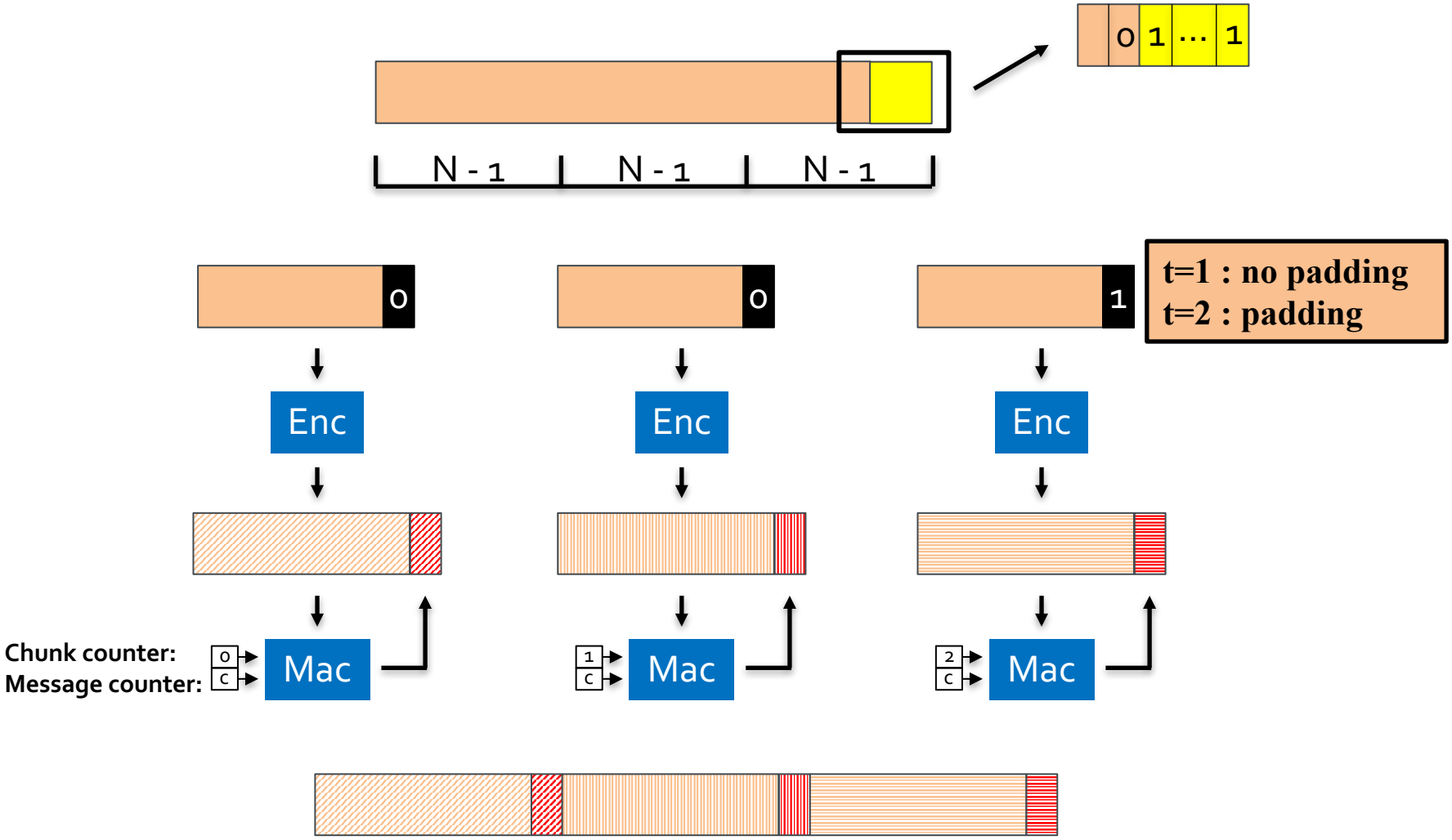
InterMAC

[BDPS12]

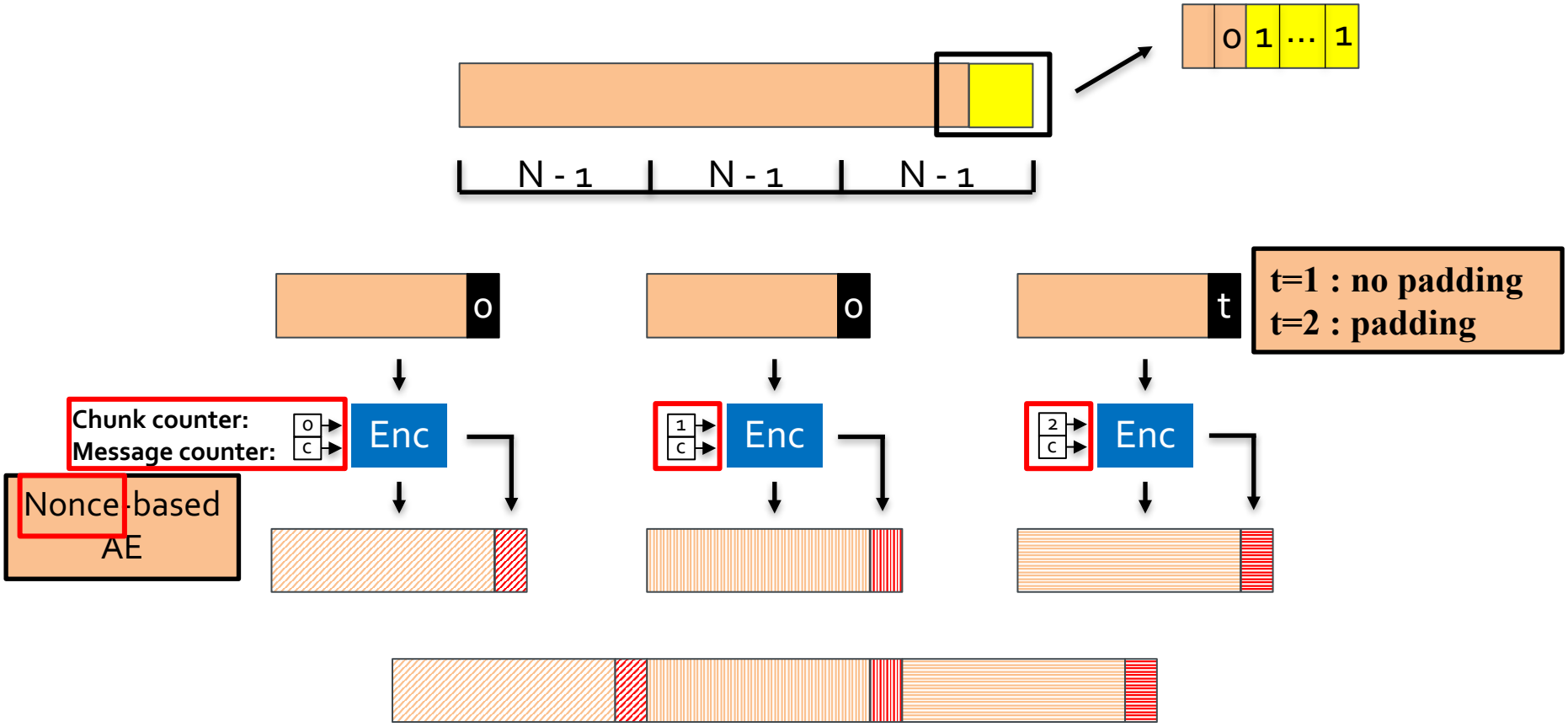
Achieve all 4 security notions



InterMAC in practice



InterMAC in practice



InterMAClib

- C-implementation
- Aims to be "safe" to use
  - Small API
  - User-oblivious nonce-management
- Algorithm agility
  - AES-GCM
  - Chacha20-Poly1305

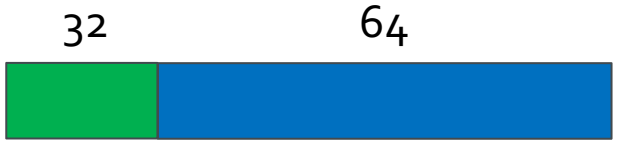
Nonce management

im_init(… , ae_cipher) :

chunk counter = 0

message counter = 0

nonce =



InterMAC with ChaCha20-Poly1305

K_{mac} <- ChaCha20(**0**, K, nonce, block_counter = 0)

rfc7539 AE construction

C <- ChaCha20(M, K, nonce, block_counter = 1)

Tag <- Poly1305(K_{mac}, C)

InterMAC with AES-GCM

Initialise aes-gcm with nonce for each chunk

We implemented InterMAC-based cipher modes in OpenSSH (v7.4)

Want cipher modes with all 4 security properties

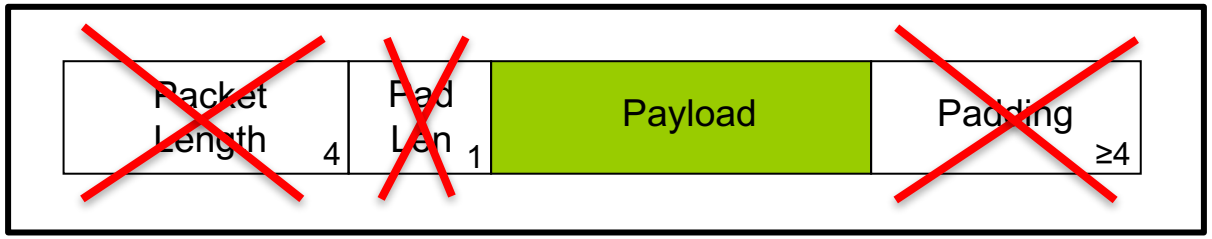
No current cipher mode satisfy that…

[ADHP16]

im-aes128-gcm-N

im-chacha-poly-N

SSH packet



Standalone code-path in the OpenSSH packet processing code

[APW09]

[PW10]

[ADHP16]

OpenSSH packet processing code: complex and buggy

Performance of InterMAC-based cipher modes compared to existing cipher modes

Throughput

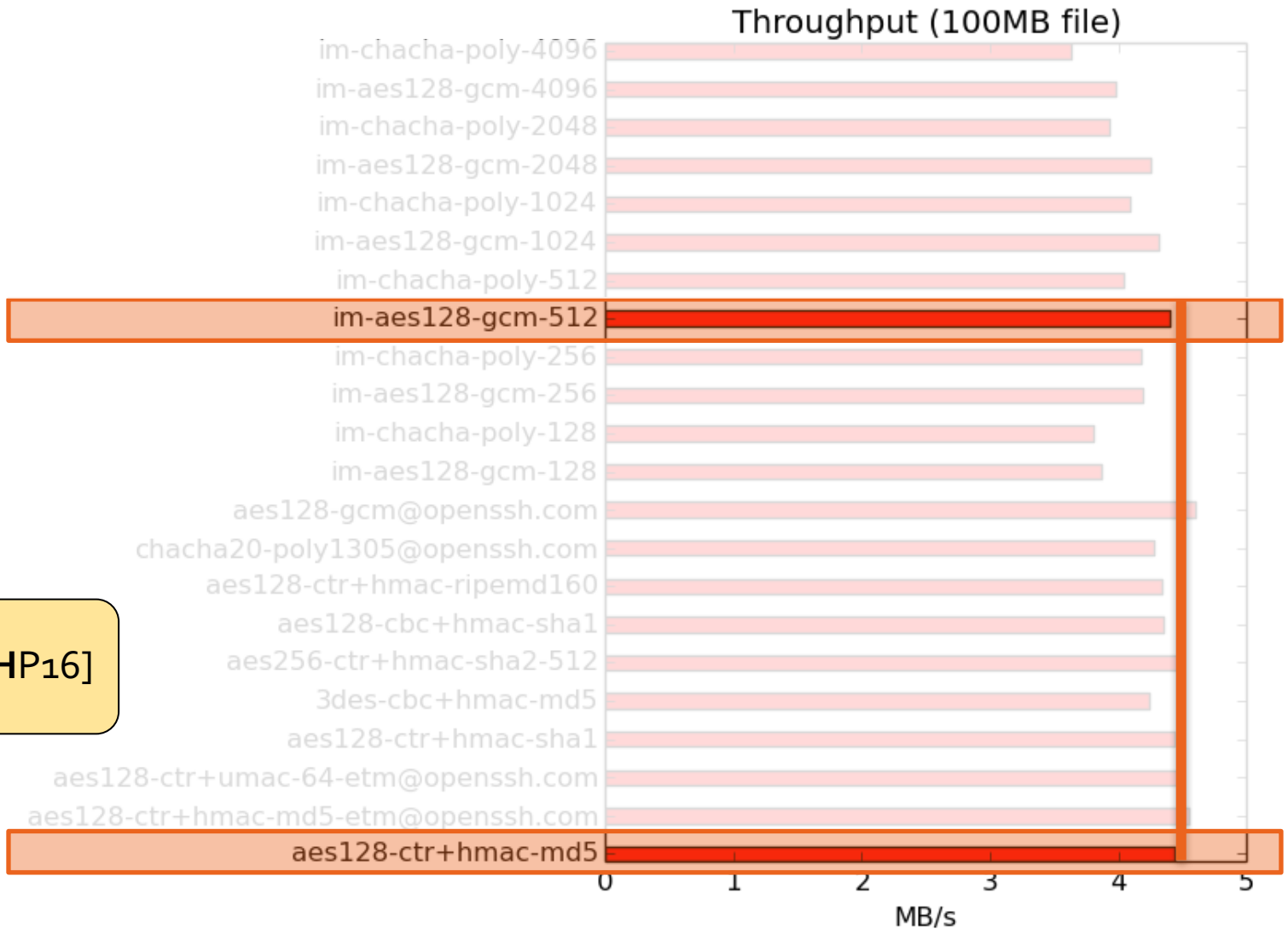
Total bytes transmitted

Behavior relating to chunk length N

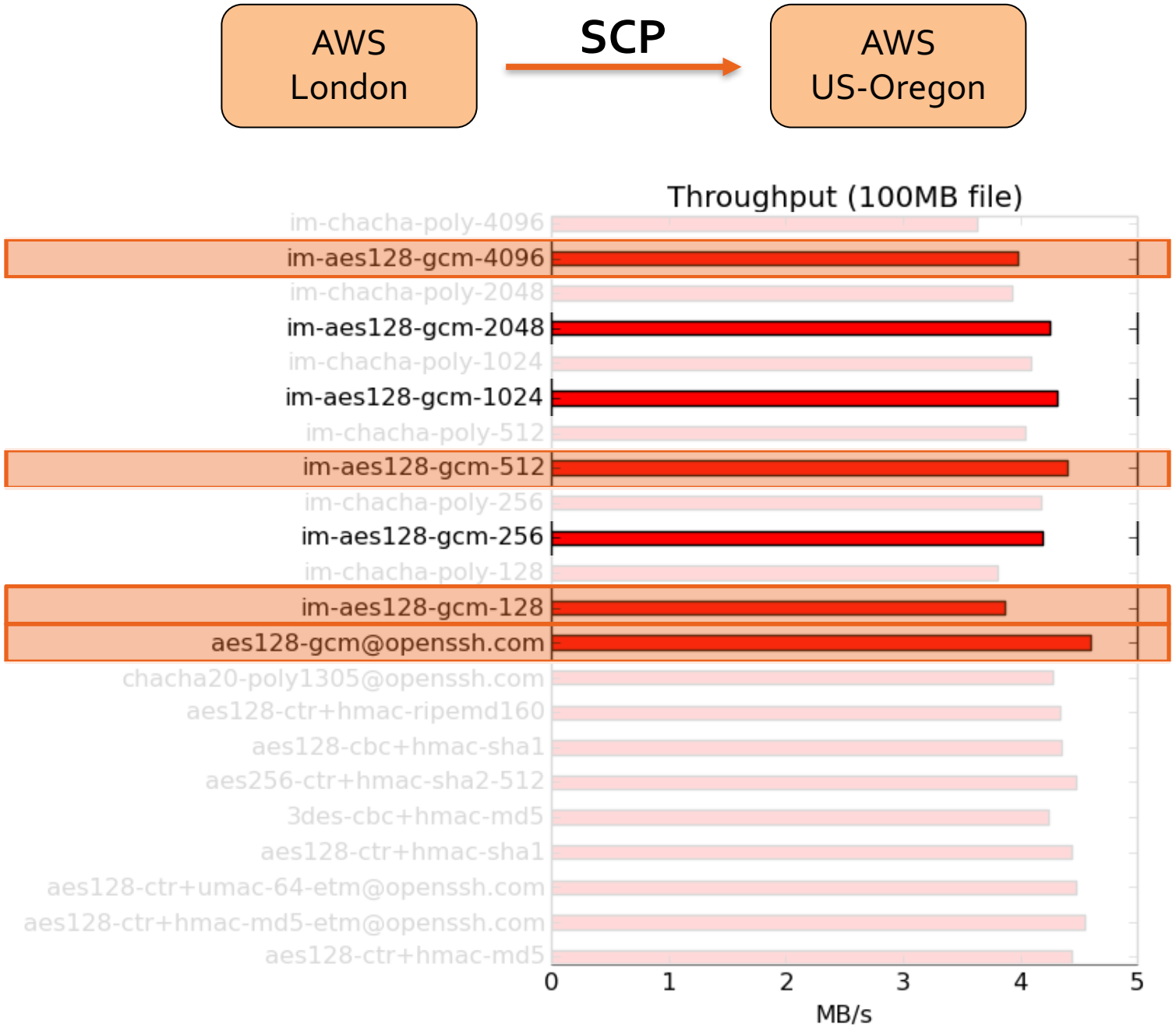
AWS London

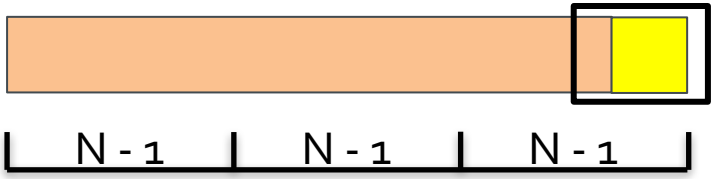
SCP →

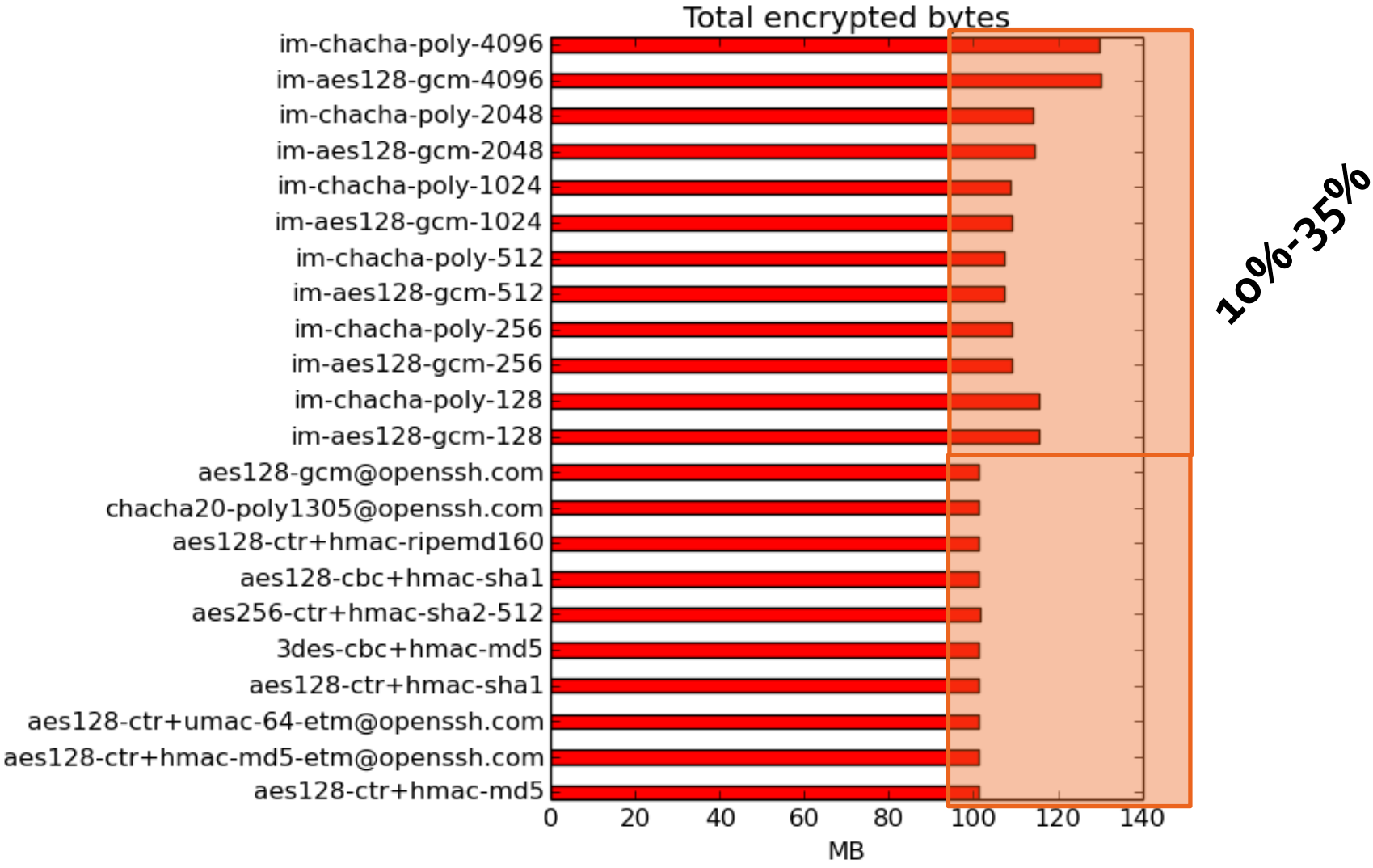
AWS US-Oregon



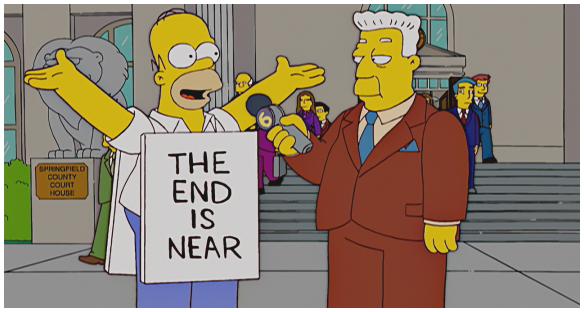
[ADHP16]


AWS
London
SCP
AWS
US-Oregon
Throughput (100MB file)
im-chacha-poly-4096
im-aes128-gcm-4096
im-chacha-poly-2048
im-aes128-gcm-2048
im-chacha-poly-1024
im-aes128-gcm-1024
im-chacha-poly-512
im-aes128-gcm-512
im-chacha-poly-256
im-aes128-gcm-256
im-chacha-poly-128
im-aes128-gcm-128
aes128-gcm@openssh.com
chacha20-poly1305@openssh.com
aes128-ctr+hmac-ripemd160
aes128-cbc+hmac-sha1
aes256-ctr+hmac-sha2-512
3des-cbc+hmac-md5
aes128-ctr+hmac-sha1
aes128-ctr+umac-64-etm@openssh.com
aes128-ctr+hmac-md5-etm@openssh.com
aes128-ctr+hmac-md5
0
1
2
3
4
5
MB/s


N - 1
N - 1
N - 1


Total encrypted bytes
im-chacha-poly-4096
im-aes128-gcm-4096
im-chacha-poly-2048
im-aes128-gcm-2048
im-chacha-poly-1024
im-aes128-gcm-1024
im-chacha-poly-512
im-aes128-gcm-512
im-chacha-poly-256
im-aes128-gcm-256
im-chacha-poly-128
im-aes128-gcm-128
aes128-gcm@openssh.com
chacha20-poly1305@openssh.com
aes128-ctr+hmac-ripemd160
aes128-cbc+hmac-sha1
aes256-ctr+hmac-sha2-512
3des-cbc+hmac-md5
aes128-ctr+hmac-sha1
aes128-ctr+umac-64-etm@openssh.com
aes128-ctr+hmac-md5-etm@openssh.com
aes128-ctr+hmac-md5
0
20
40
60
80
100
120
140
MB
10%-35%

Finish line is in sight…



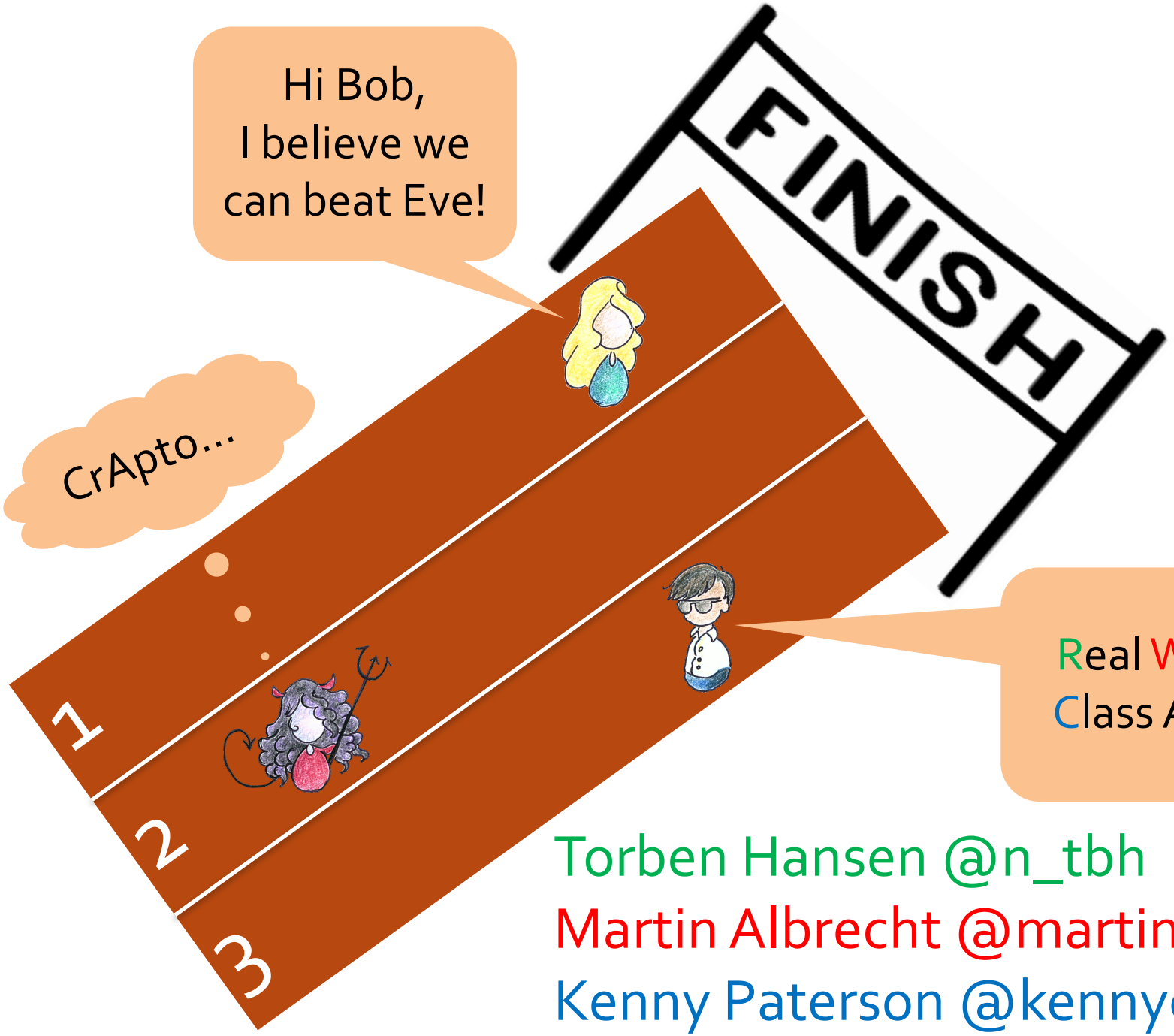
Implementations must cater for ciphertext fragmentation

We believe this feature should be reflected in the security models → [BDPS12] provides a security model for studying symmetric encryption schemes supporting ciphertext fragmentation

InterMAC satisfies all security notions from [BDPS12] → We modify InterMAC to make it usable in practice and create InterMAClib

OpenSSH want cipher modes that meets all security notions from [BDPS12] → We implement InterMAC-based cipher modes in OpenSSH using InterMAClib

InterMAC: SSH binary packet protocol done right, using modern primitives → We measured performance; indicates that greater security can be traded for only a minor performance hit



Torben Hansen @n_tbh
Martin Albrecht @martinralbrecht
Kenny Paterson @kennyog