AEGIS
Fast Authenticated Encryption Family

F. Denis (Fastly Inc.), F.E.R. Scotoni, S. Lucas,
C. Fruhwirth (Google), D. Bleichenbacher (Google)
B. Preneel (Univ. of Leuven),
H. Wu (Nanyang Technological Univ.)

CFRG @IETF113

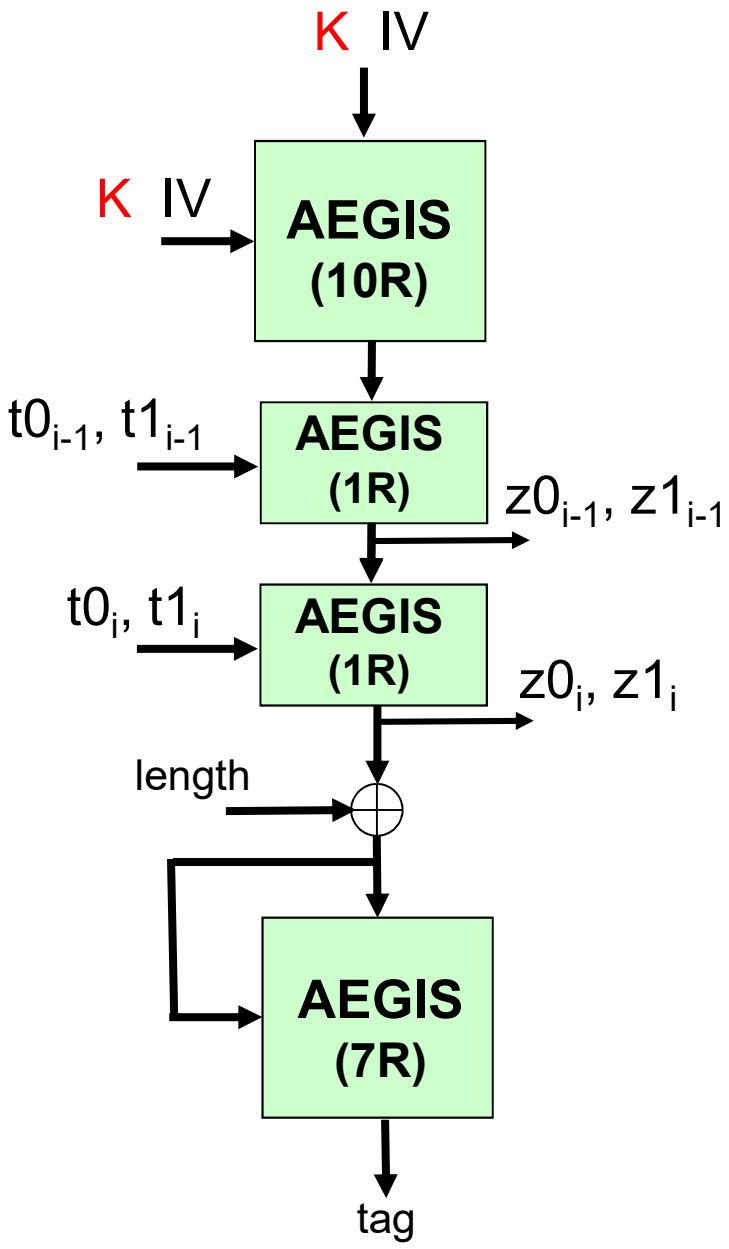
The AEGIS family of authenticated encryption algorithms

draft-denis-aegis-aead-03 – 6 March 2022

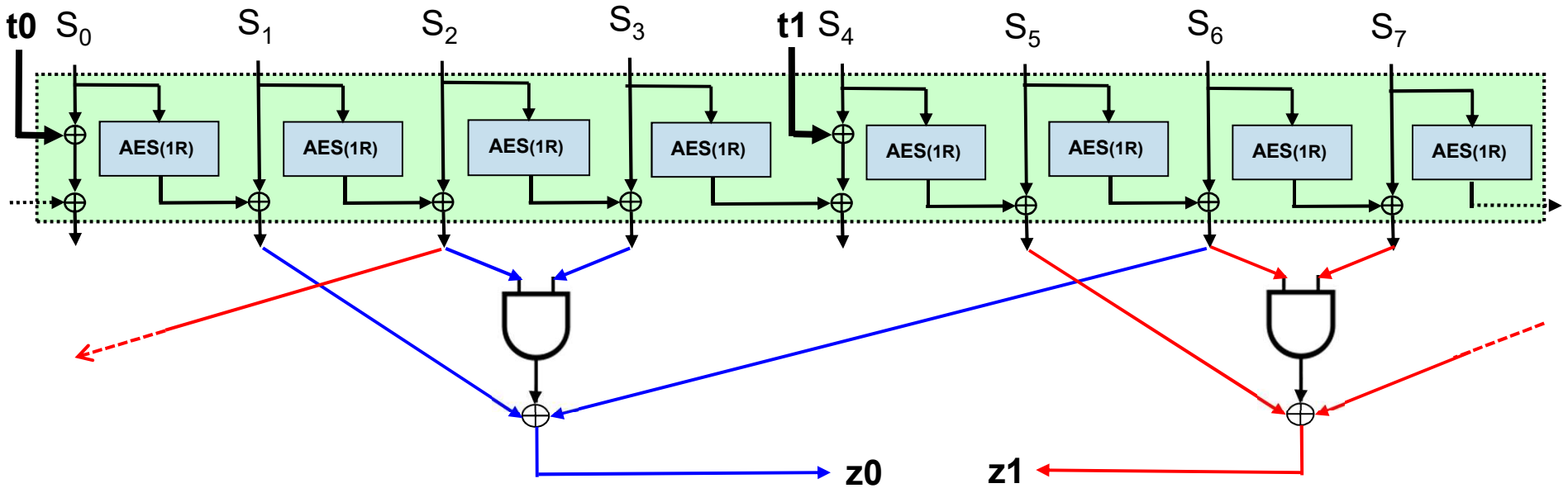
- nonce-based Authenticated Encryption
- 2x faster than AES-GCM: 0.287 cycles/byte
- high security level
- multiple implementations available (including in Linux kernel)

Design: AEGIS-128L

- K, IV (nonce), data words, tag: 128 bits
- large state: 8 x 128 bits
- modular
- easy to analyze
- create stream cipher from MAC algorithm



Design: AEGIS-128L (2/2): 1 round



- Accepts 2 128-bit plaintext words t0, t1
- Updates 7x128-bit state S0,…S7
- Non-linear output function produces 2 128-bit words z0 and z1
- Ciphertext = to ⊕ zo ; t1 ⊕ z1

Security properties

Nonce-based authenticated encryption with associated data

	confidentiality	data authentication (forgery)
AEGIS-128L	2^{128}	2^{128}
AEGIS-256	2^{256}	2^{128}

AEGIS-128L:

per key 2^{48} messages (each with different nonce)

AEGIS-256:

no practical restriction on # messages/key

key recovery faster than 2^{256} possible after 2^{128} online forgery attempts

AEGIS security properties

- Key committing: cannot generate a ciphertext that successfully decrypts under multiple keys
- Nonce: length can be freely chosen ([0,128] or [0,256])

Not

- resistant to nonce reuse
- allowed to release unverified plaintext
- compactly committing: same ciphertext can be successfully decrypted under multiple keys

Inherent if speed > AES & 128-bit tag

AEGIS: independent security evaluation

- AEGIS-128 in final portfolio of CAESAR competition (2014-2018) http://competitions.cr.yp.to/caesar.html
- [Minaud, SAC 2014][Eichlseder+ FSE 2020]
  - Correlation in keystream if $2^{152}..2^{162}$ ciphertexts are available for AEGIS-256 (purely certificational)
- Attacks on reduced round initialization of AEGIS-128
  - [Liu+, FSE 2022] – does not apply to schemes in draft
    - 5/10 rounds: 2^{96} weak keys that can be recovered in time 2^{72}
  - [SHI+22, Chinese J. Electronics]
    - 4/10 rounds: key recovery 2^{34} IV queries in time 2^{30} and memory 2^{30}

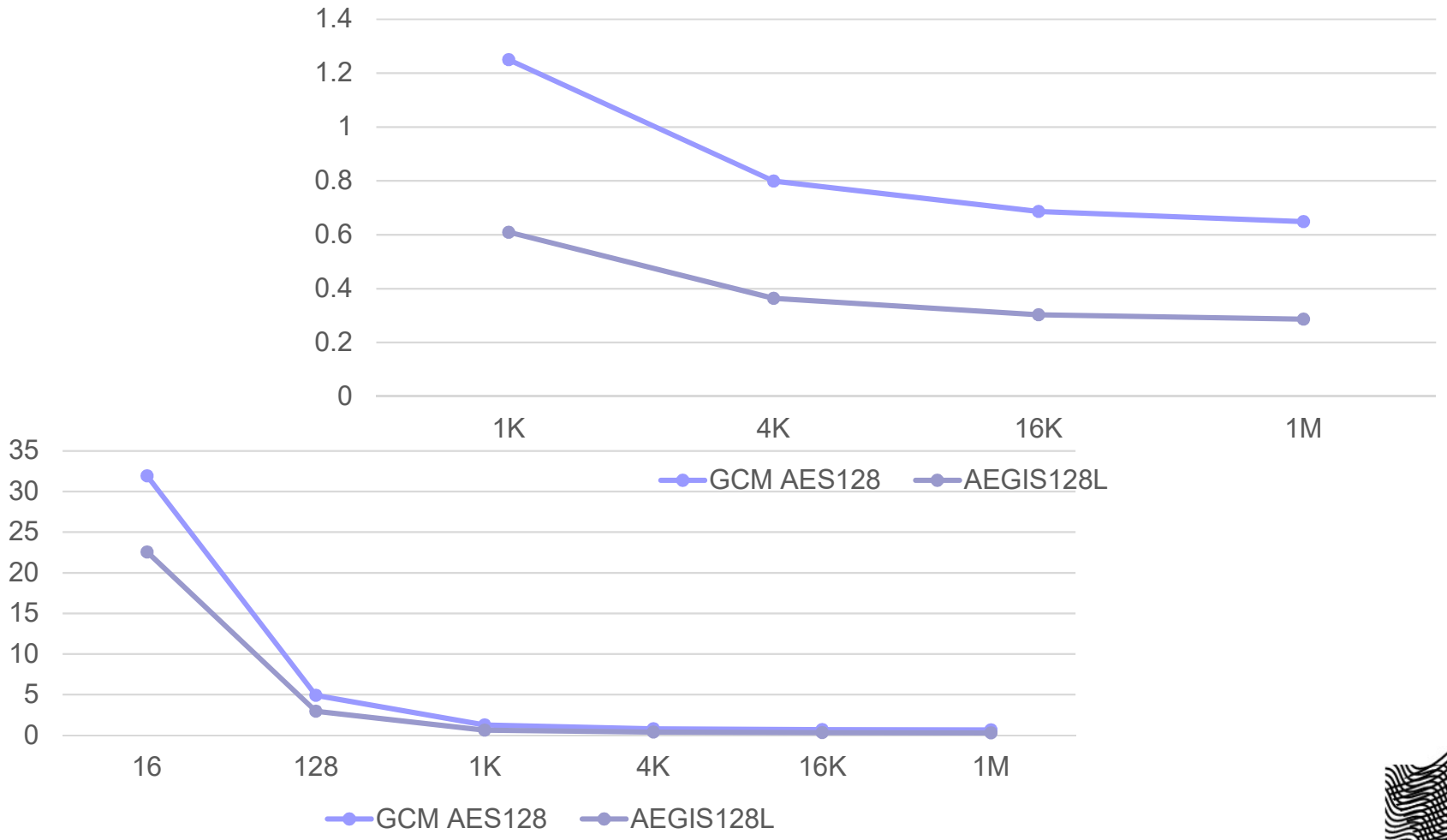
AEGIS performance

- Parallelizable
- Online for encryption
- Optimal use of AES hardware support

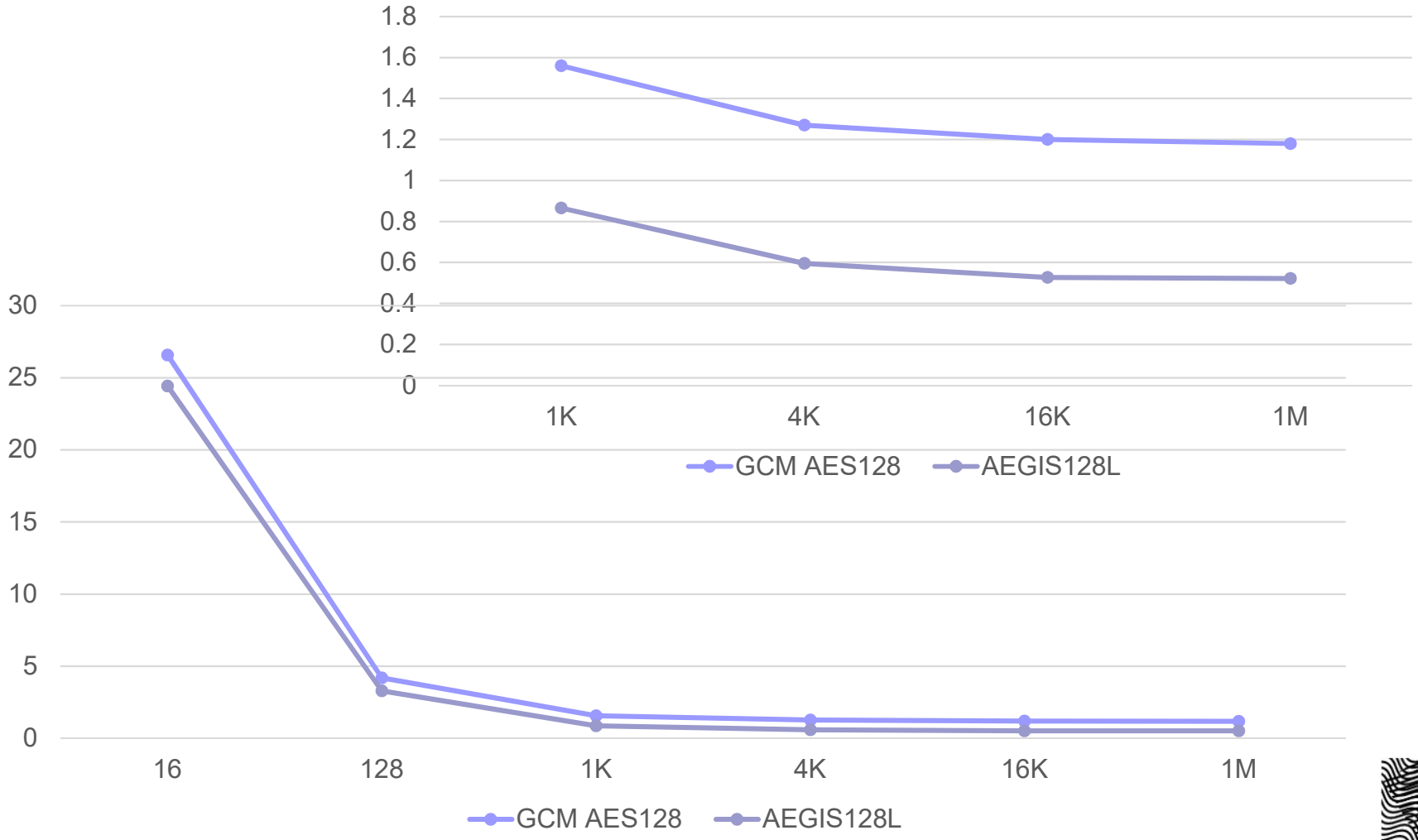
Next slides: comparison

- AEGIS128L
  https://github.com/google/aegis_cipher
- AES-128-GCM from BoringCrypto:
  https://boringssl.googlesource.com/boringssl/

Intel Skylake Xeon with HyperThreading (3 cores) dL1:32KB dL2:1024KB dL3:8MB (3696 MHz) cycles/byte



ARM Neoverse N1 (64 cores) (3000 MHz) (cycles/byte)



Conclusion: AEGIS

- Simple design for 128-bit and 256-bit security
- Ultra fast for protecting network packets
  - targeting platform with AES hardware support
  - without this support, AEGIS is faster than plain AES (factor 1.25-2)
- High level of security