irtf-cfrg-aegis-aead

The AEGIS Family of Authenticated Encryption Algorithms

Frank DENIS, Fastly for IETF 117

AEGIS

- Nonce-respecting Authenticated Encryption with Associated Data
- Can also be used as a high-performance, strong MAC
- Optimized for CPUs with AES pipelines
- Better security bounds than AES-GCM
- Key committing
- Large nonce size (128 or 256 bits)
- Non-invertible state
- Simple to implement safely and efficiently

Updates between -00 and -04

- Addressed all the feedback we received from CFRG members and implementers
- Original constructions unchanged
- New analysis confirms that AEGIS with the specified parameters has a comfortable security margin
- Authentication tags can now be 128 or 256 bits. Larger tags improve key commitment and collision resistance
- Additional test vectors
- Documented usage with TLS, DTLS and QUIC
- IANA entries in the AEAD Algorithms and TLS Cipher Suites registries

Implementations

Name	Language
This document's reference implementations	Zig
CAESAR reference AEGIS-128L implementations	C
CAESAR reference AEGIS-256 implementations	C
Linux kernel	C
libsodium	C
angt/aegis256	C
TwoEightNine/aegis	C
libaegis	C
Experimental support for BoringSSL	C, C++
google/aegis-cipher	C++
aegis	Rust
Zig standard library	Zig
x13a/py-aegis	Python
ericlagergren/aegis	Go
samuel-lucas6/AEGIS.NET	C#
Aegis-js	JavaScript
Aegis-kotlin	Kotlin

Real-world usage

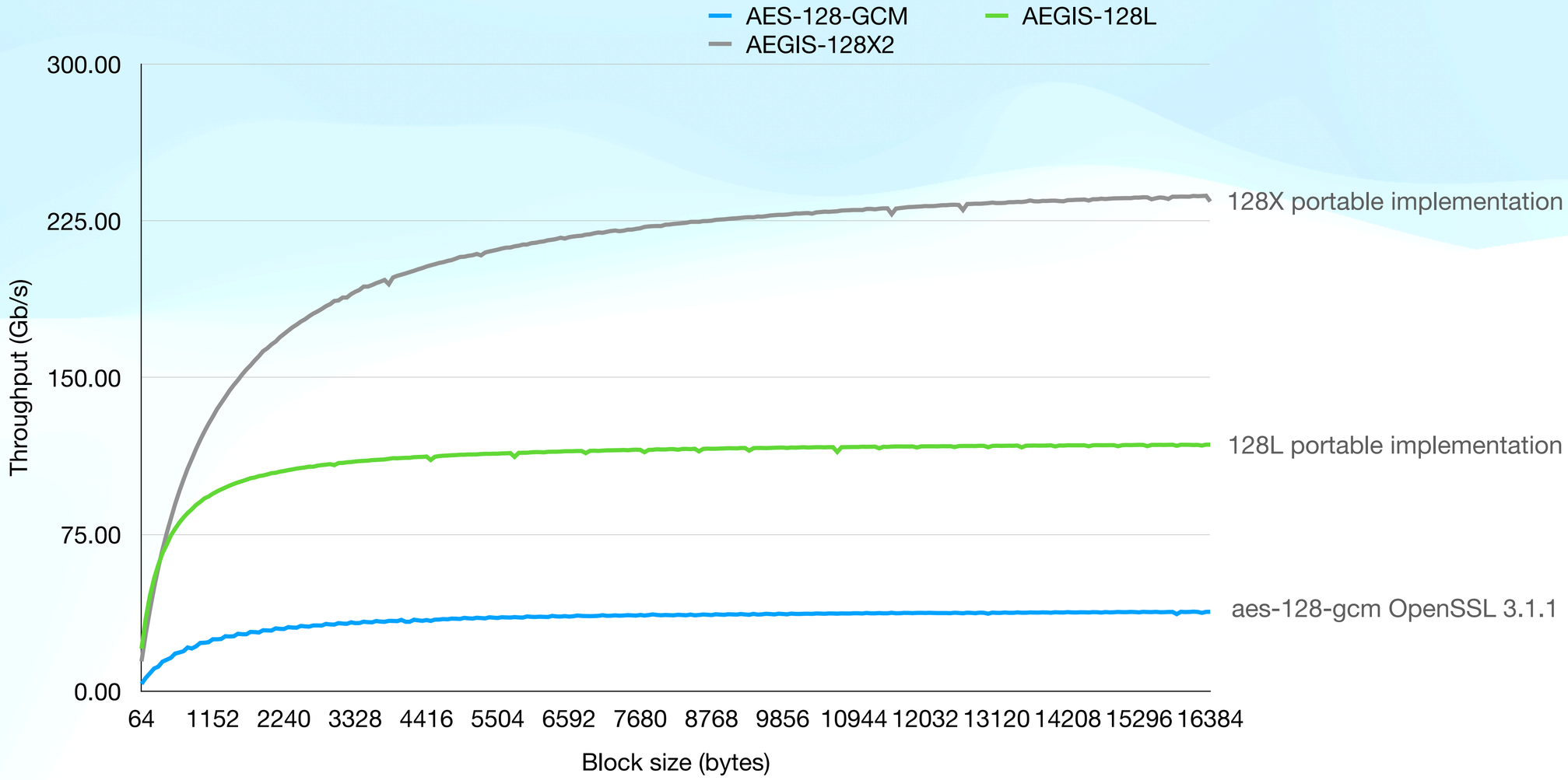
- Tigerbeetle financial database
- Linux kernel (dm-crypt)
- Zig standard library TLS 1.3 implementation
- Used internally at OVH, Google and Fastly for performance critical applications

AEGIS-128X and AEGIS-256X

- Optional variants of AEGIS for CPUs with vector AES instructions
- Simple parallel modes on top of AEGIS-128L and AEGIS-256
- Easy to implement
- Same usage and same security properties as AEGIS-128L and AEGIS-256
- Efficient even with short messages

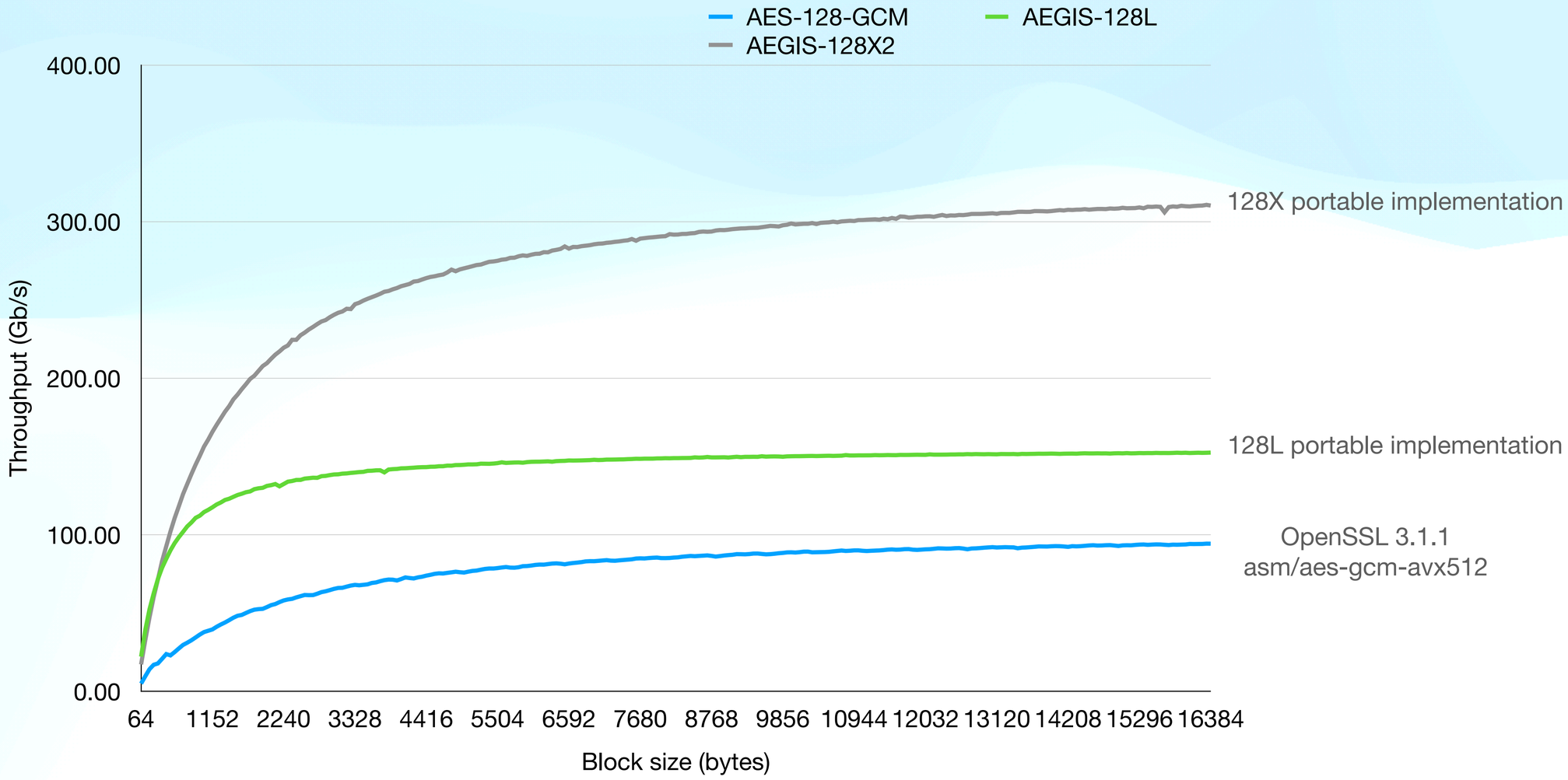
AEGIS-128X

AMD Epyc 7543 (AVX2+VAES)



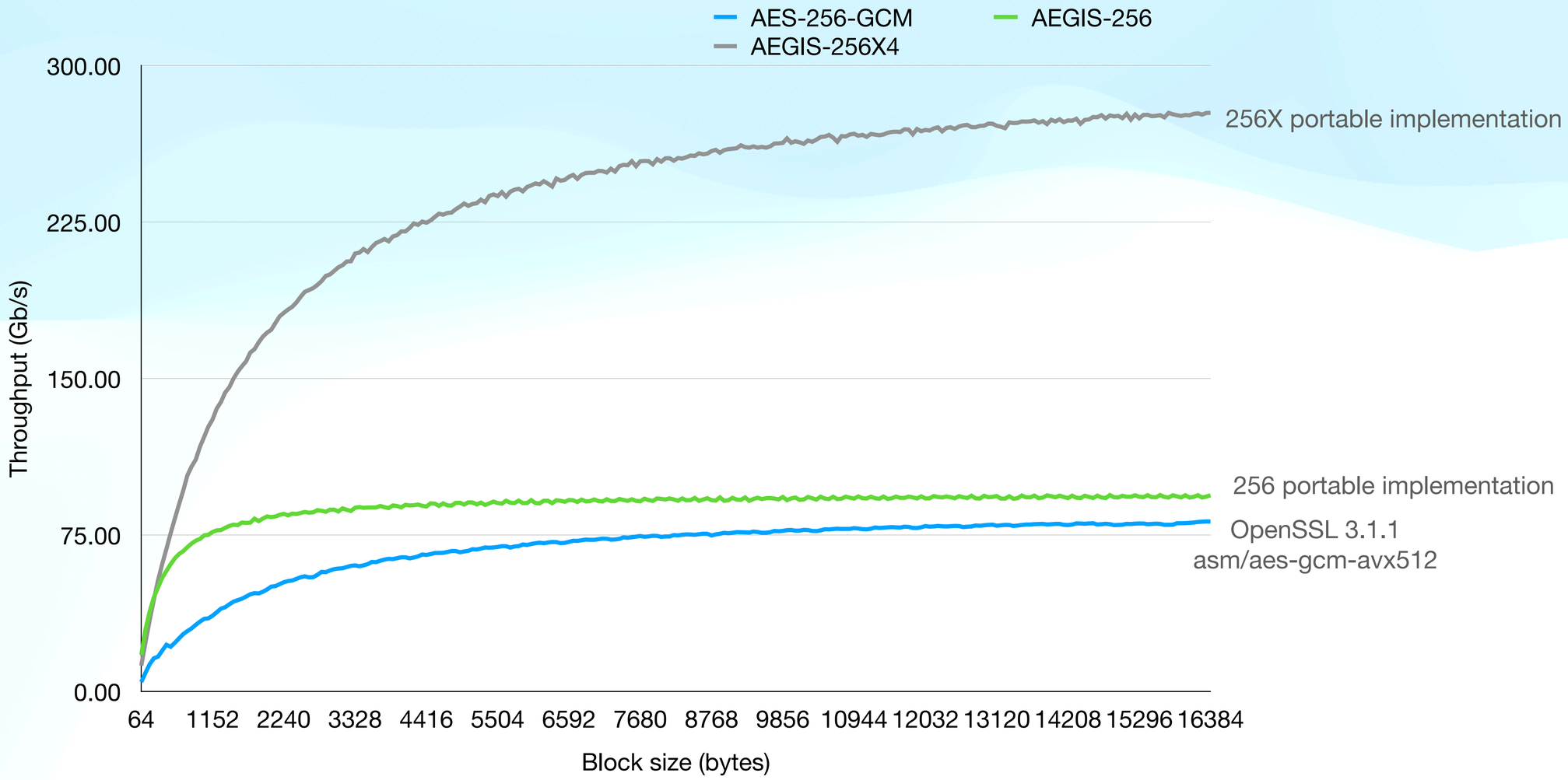
AEGIS-128X

AMD Ryzen 7 7700 (AVX512+VAES)



AEGIS-256X

AMD Ryzen 7 7700 (AVX512+VAES)



Next

- AEGIS-128X and 256X will be included in the next revision of the draft
- No other changes planned to the set of algorithms nor to their parameters.

Thank you!

https://datatracker.ietf.org/doc/draft-irtf-cfrg-aegis-aead/