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

<table>
<thead>
<tr>
<th>Name</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>This document’s reference implementations</td>
<td>Zig</td>
</tr>
<tr>
<td>CAESAR reference AEGIS-128L implementations</td>
<td>C</td>
</tr>
<tr>
<td>CAESAR reference AEGIS-256 implementations</td>
<td>C</td>
</tr>
<tr>
<td>Linux kernel</td>
<td>C</td>
</tr>
<tr>
<td>libodium</td>
<td>C</td>
</tr>
<tr>
<td>angt/aegis256</td>
<td>C</td>
</tr>
<tr>
<td>TwoEightNine/aegis</td>
<td>C</td>
</tr>
<tr>
<td>libaegis</td>
<td>C</td>
</tr>
<tr>
<td>Experimental support for BoringSSL</td>
<td>C, C++</td>
</tr>
<tr>
<td>google/aegis-cipher</td>
<td>C++</td>
</tr>
<tr>
<td>aegis</td>
<td>Rust</td>
</tr>
<tr>
<td>Zig standard library</td>
<td>Zig</td>
</tr>
<tr>
<td>x13a/py-segis</td>
<td>Python</td>
</tr>
<tr>
<td>ericlagergren/aegis</td>
<td>Go</td>
</tr>
<tr>
<td>samuel-lucasp/AEGIS.NET</td>
<td>C#</td>
</tr>
<tr>
<td>Aegis-js</td>
<td>JavaScript</td>
</tr>
<tr>
<td>Aegis-kotlin</td>
<td>Kotlin</td>
</tr>
</tbody>
</table>
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)

Throughput (Gb/s)

Block size (bytes)
AEGIS-256X
AMD Ryzen 7 7700 (AVX512+VAES)

Throughput (Gb/s)

Block size (bytes)

256X portable implementation

256 portable implementation

OpenSSL 3.1.1
asm/aes-gcm-avx512

AES-256-GCM
AEGIS-256X4
AEGIS-256
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!