IETF Hackathon

IETF 123
19–20 July 2025
Madrid, Spain

HiAE

Why a new authenticated encryption algorithm?

- Encryption and authentication are critical to many IETF projects.
- Performance has also become critical as bandwidth and data usage requirements grow.
- Recent ultra-fast ciphers for software implementations appeared, but they were primarily designed for Intel CPUs
- However, ARM CPUs become increasingly prevalent, both in mobile devices and computers.
- **HiAE** was specifically designed to be extremely fast on

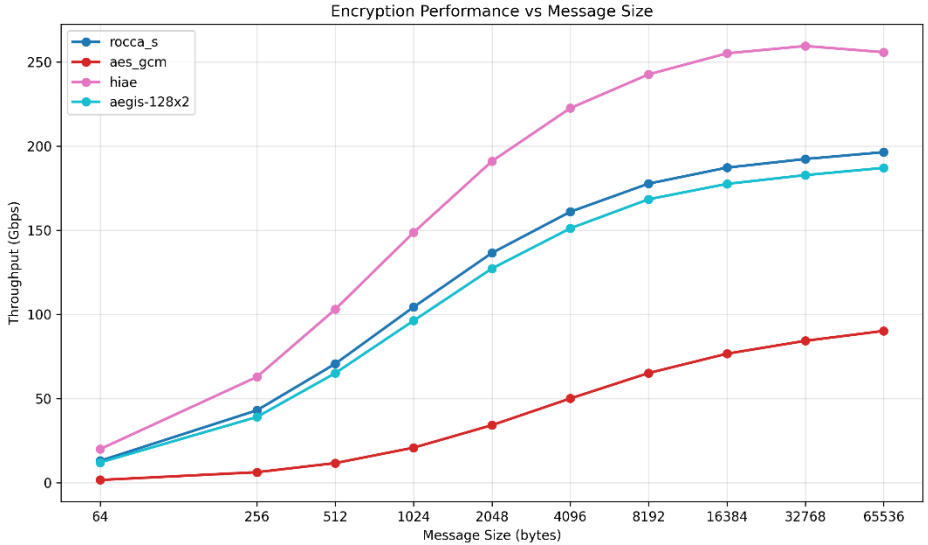
Hackathon Plan

- Problem: Evaluating the performance of **HiAE – High throughput authenticated encryption** on ARM and x86
  - Draft: draft-pham-cfrg-hiae

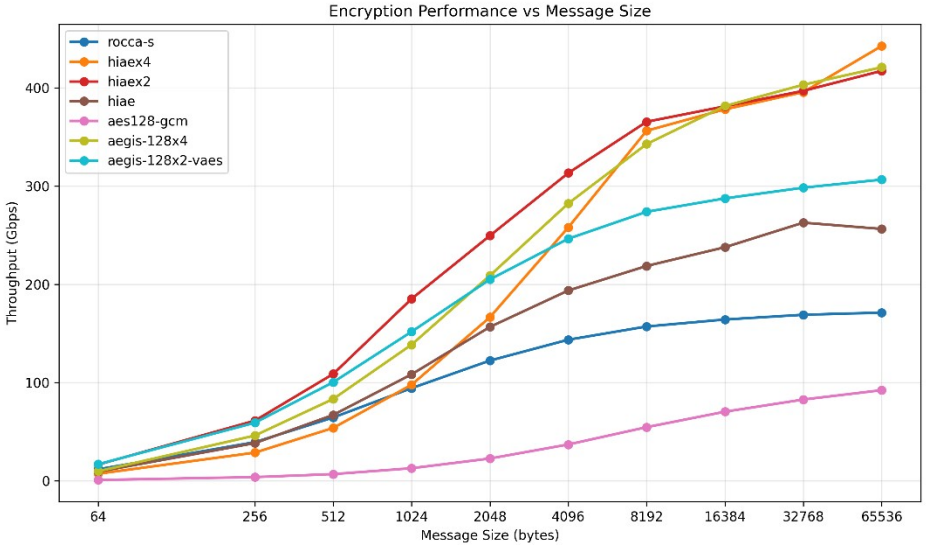
What got done

- **draft-pham-hiae:** comprehensive, complete draft specification for users and implementers.
- Implementations in Python, C, Zig, Rust, JavaScript and Go.
- **Performance** of the reference implementation was improved by 23%
- Parallel versions for Intel CPUs were designed and implemented
- **Multi-platform benchmarks**, including comparisons other recent high-performance ciphers (AEGIS, ROCCA-S).

What got done



Apple M4



AMD Zen 4

Wrap Up

Team members:

Frank Denis
fdenis@fastly.com
Phuong Pham
pham.phuong@huawei.c
Lucas Prabel
lucas.prable@huawei.com
Shuzhou Sun
sunshuzhou@huawei.com

HiAE

Link: https://github.com/hiae-aead/draft-pham-hiae/