IETF Hackathon
Rocca-S in parallel mode

IETF 124
1–2 November 2025
Montreal, Canada

I E T F

Background: Rocca-S

Rocca-S is a very fast 256-bit symmetric key encryption algorithm

- Design
  - Sponge-based construction
  - 256-bit key and 256-bit tag
  - Three modes: AEAD, encryption only and keystream generation
- Security (in nonce respecting setting)
  - Classical setting: 256-bit security against key-recovery and 192-bit security against forgery
  - Quantum setting: 128-bit security against key-recovery and forgery
- Internet draft: https://datatracker.ietf.org/doc/draft-nakano-rocca-s/
- The paper is presented at ESORICS 2023

Hackathon Plan

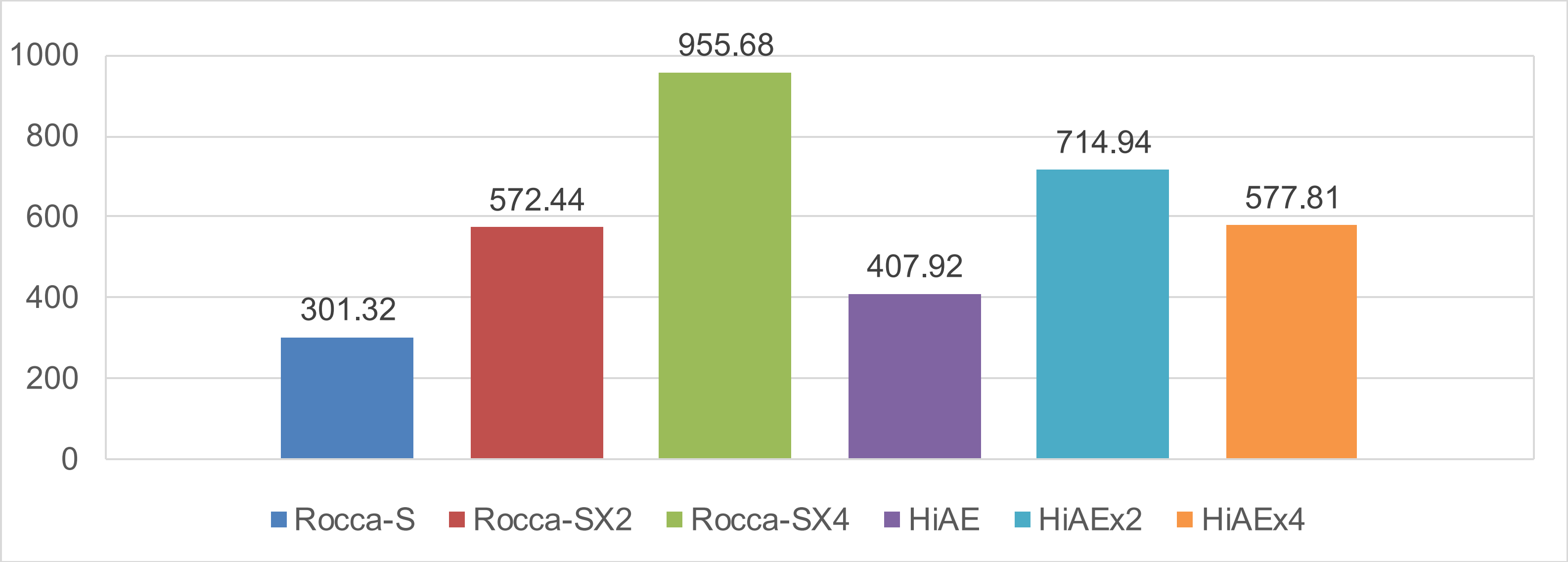
- CPUs with AVX-512 support the instruction set for executing multiple AES round functions in parallel
- Implement Rocca-S in parallel mode with AVX-512 to achieve higher throughput

What got done

- Implemented Rocca-SX2 (two parallelized version) and Rocca-SX4 (four parallelized version)
- Used HiAE benchmark (https://github.com/hiae-aead/benchmarks) for performance evaluation

What we learned

- Rocca-SX2 achieves 572.44Gbps and Rocca-SX4 achieves 955.68Gbps on AMD Ryzen 9 9900X



Wrap Up

Team members:

First timers @ IETF/Hackathon:

The detail of parallel mode will be specified in the new version of the draft: https://datatracker.ietf.org/doc/draft-nakano-rocca-s/

The implementation will be uploaded to github: https://github.com/yt-nakano

Acknowledgement

This activity is partially supported by a contract of "Research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)", which was supported by the Ministry of Internal Affairs and Communications, Japan.