IETF Hackathon

IETF 121
2–3 Nov 2024
Dublin, Ireland

Rocca-S

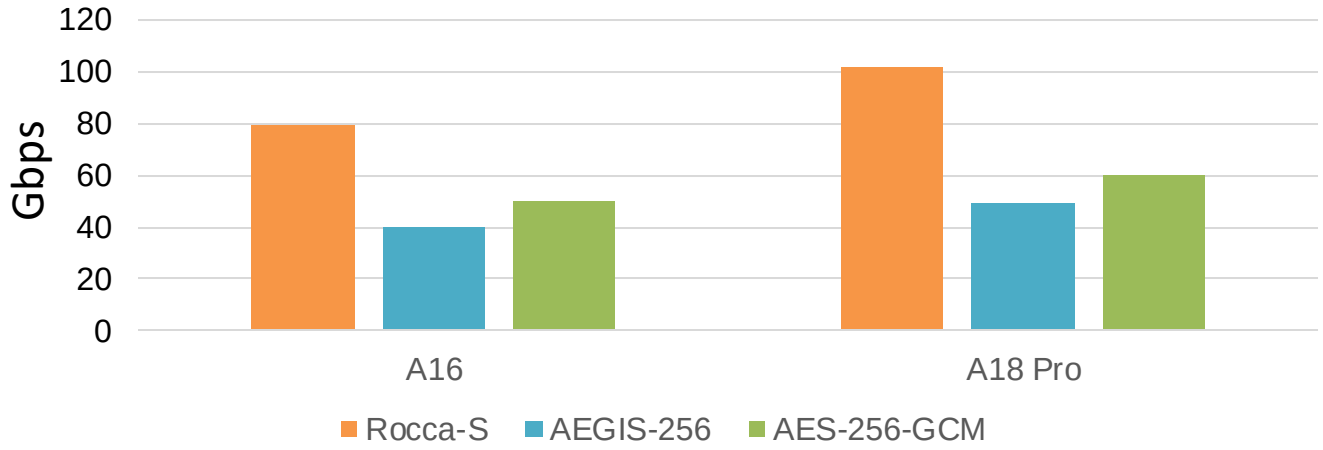
- Design
  - Sponge-based construction
  - 256-bit key and 256-bit tag
  - Three modes: AEAD, encryption only and keystream generation
- Security (in nonce respecting setting)
  - Classical setting: 256-bit security against key-recovery and 192-bit security against forgery
  - Quantum setting: 128-bit security against key-recovery and forgery
- Internet draft: https://datatracker.ietf.org/doc/draft-nakano-rocca-s/
- Implementations: https://github.com/yt-nakano/
  - Including the result of IETF #118 hackathon (quictls+Rocca-S)
- The paper is presented at ESORICS 2023

Hackathon Plan

- Implement Rocca-S for mobile phones for performance evaluation
  - Use openssl as a base and include ciphers
  - Use ‘openssl speed -aead’ to measure the throughput

What got done

- Verified the performance advantage of Rocca-S to other algorithms
- Rocca-S achieved 102Gbit/s



Wrap Up

Team members:

Yuto Nakano

First timers @ IETF/Hackathon:

Email: yt-nakano[at]kddi.com

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.