Rocca-S

Yuto Nakano

Rocca-S

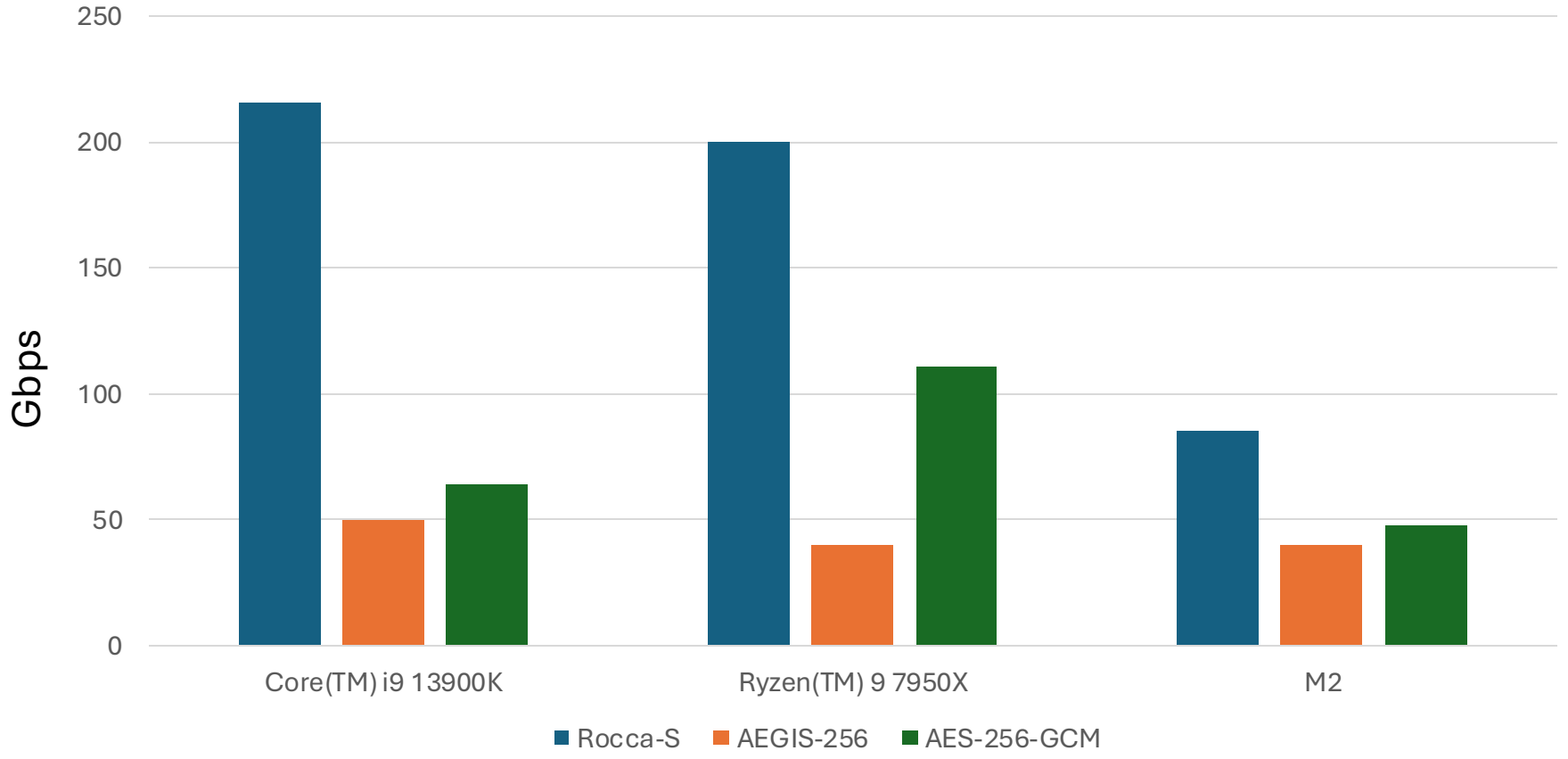
- Design
  - Sponge-based construction
  - 256-bit key and 256-bit tag
  - Three modes: AEAD, encryption only and keystream generation
- Security (in nonce respecting setting)
  - Classical setting: 256-bit security against key-recovery and 192-bit security against forgery
  - Quantum setting: 128-bit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

Opensource

- Several implementations are available including
  - openssl
  - quictls+msquic (achievement in IETF #118 hackathon)
  - libsodium
  - reference implementation
- Link to github is https://github.com/yt-nakano

Performance evaluation update

- Performance evaluation with “openssl speed -aead”



Potential use cases requiring high throughput

- High Performance Wide Area Network (hp-wan)
  - Massive data transmission between data centres with data integrity
- 6G discussion in 3GPP
  - 3GPP SA1 is now discussing new use cases and their requirements for 6G
    - System and Operational Aspects
    - Integrated Sensing and Communication
    - Ubiquitous Connectivity
    - **Immersive Communication** (which requires high throughput)
    - Massive Communication
    - Further Use Cases on Industry and Verticals
- 6G white papers from various organisations
  - Holography, digital twin, big data analytics
- Other use cases
  - Massive IoT/drone platform
  - Inter-GPU communication for AI (GPU cluster)
  - High-quality real-time medical data transmission

Discussion

- Would you support the adoption of Rocca-S as a CFRG item?

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.