Encryption Algorithm Rocca-S

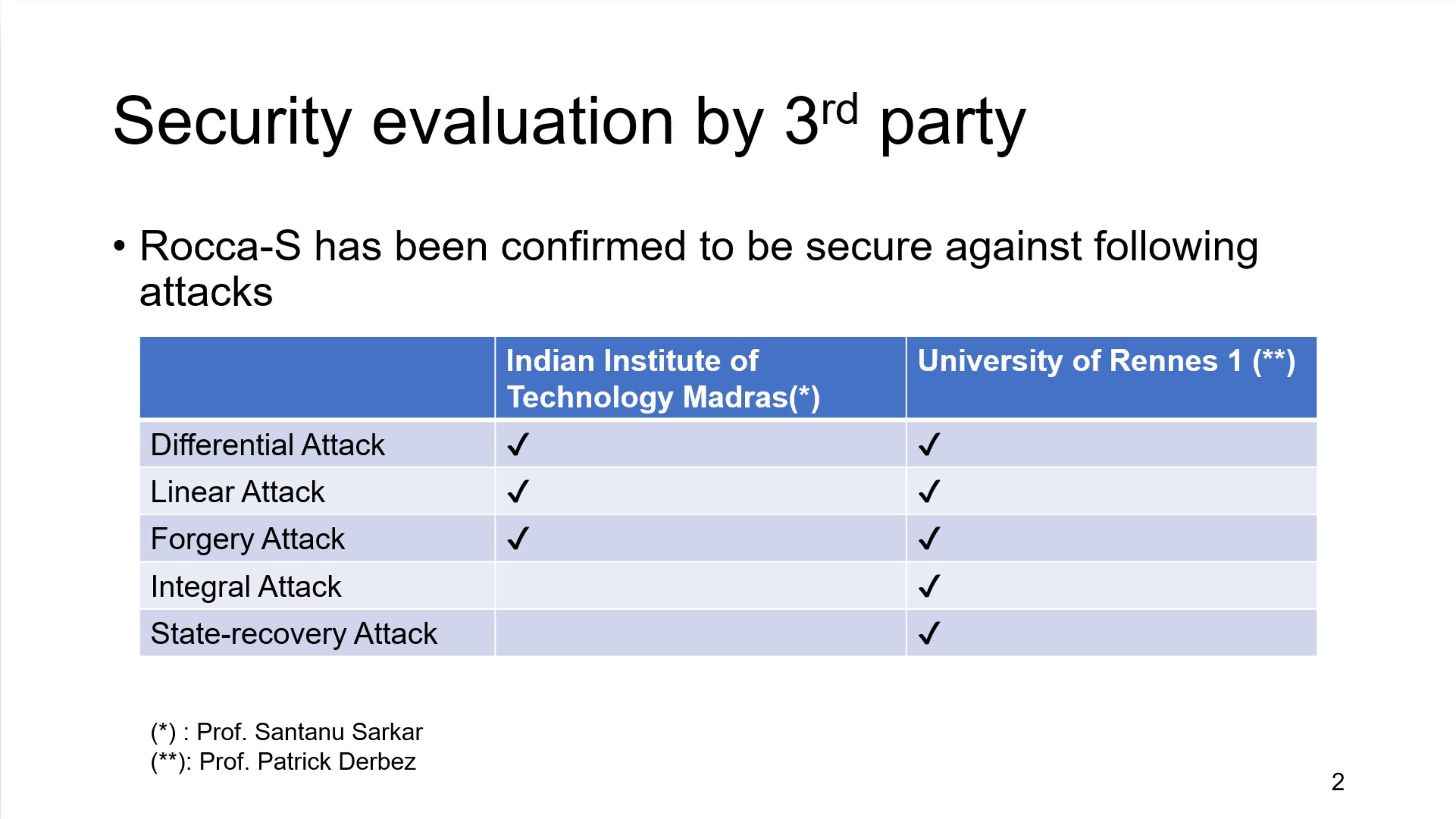
Yuto Nakano

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

Security evaluation by 3rd party

(presented at IETF 116)



Security evaluation by 3rd party

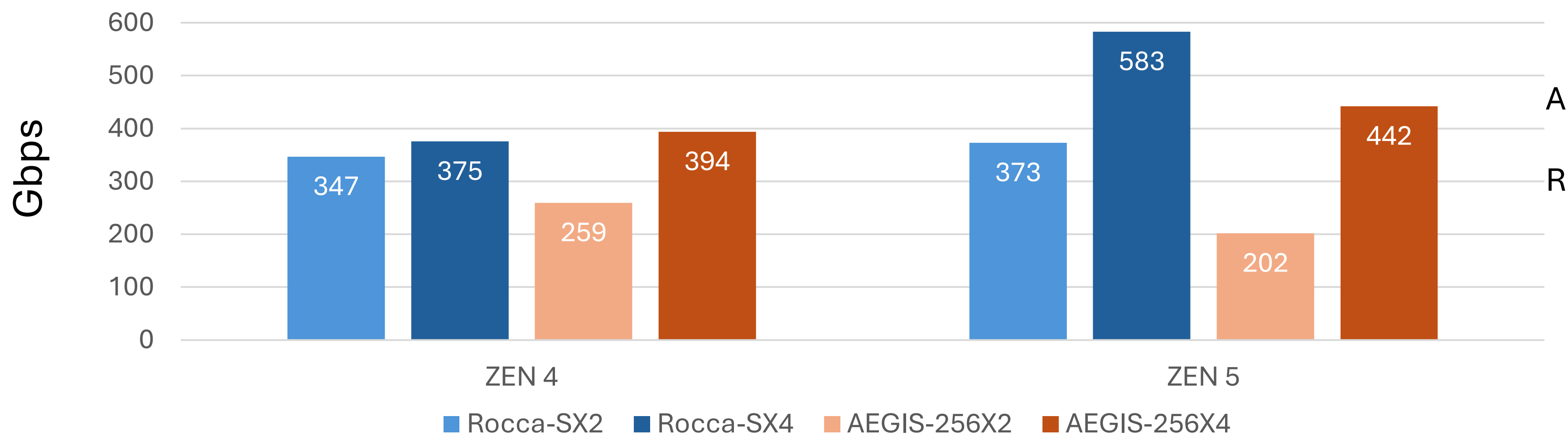
- Rocca-S has been confirmed to be secure against following attacks

	Indian Institute of Technology Madras(*)	University of Rennes 1 (**)
Differential Attack	✓	✓
Linear Attack	✓	✓
Forgery Attack	✓	✓
Integral Attack		✓
State-recovery Attack		✓

(*) : Prof. Santanu Sarkar
(**): Prof. Patrick Derbez

Rocca-SX

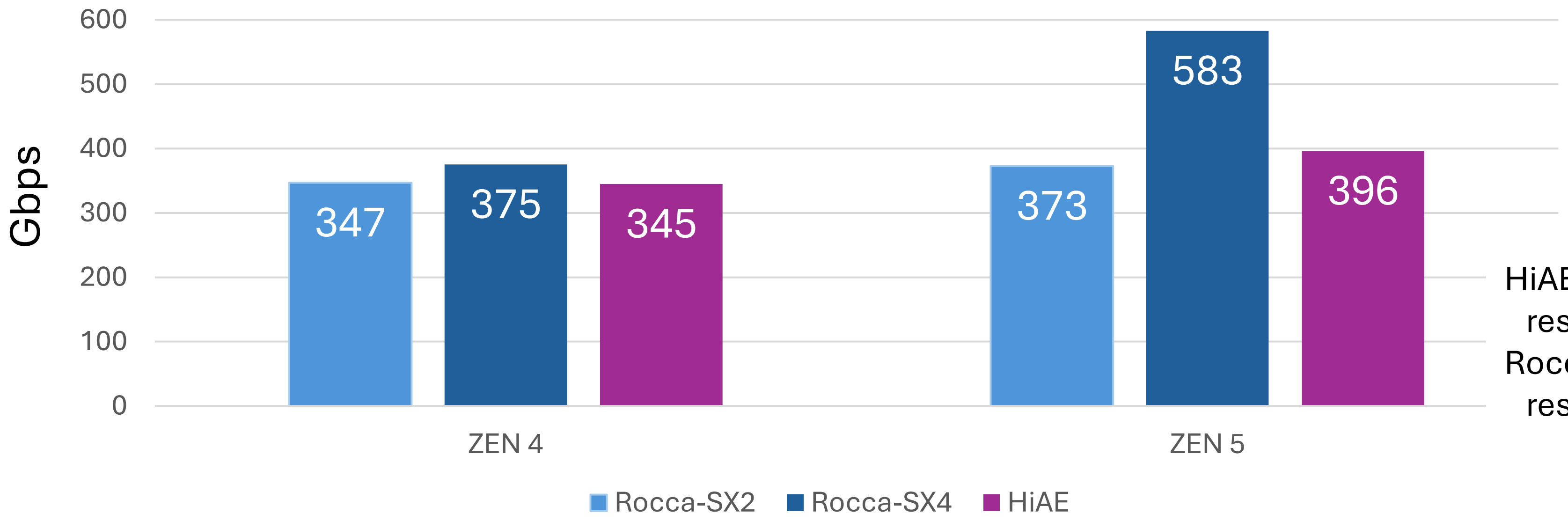
- Parallel modes of Rocca-S for higher performance
  - Rocca-SX2: 2 parallel lanes
  - Rocca-SX4: 4 parallel lanes
  - Same construction as AEGIS-256X2 and AEGIS-256X4
- Performance comparison with AEGIS family



AEGIS family:
results using libaegis benchmark
Rocca-S family:
results using “openssl speed -aead”

Comparison with HiAE

- HiAE is another AEAD aiming high throughput
- HiAE requires 2048-bit of internal state, which is similar to 1792-bit of Rocca-SX2



HiAE:
  results using official benchmark
Rocca-S family:
  results using "openssl speed -aead"

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.