Encryption algorithm Rocca-S
draft-nakano-rocca-s

Yuto Nakano, Kazuhide Fukushima, Takanori Isobe

CRFG@IETF115

Backgrounds

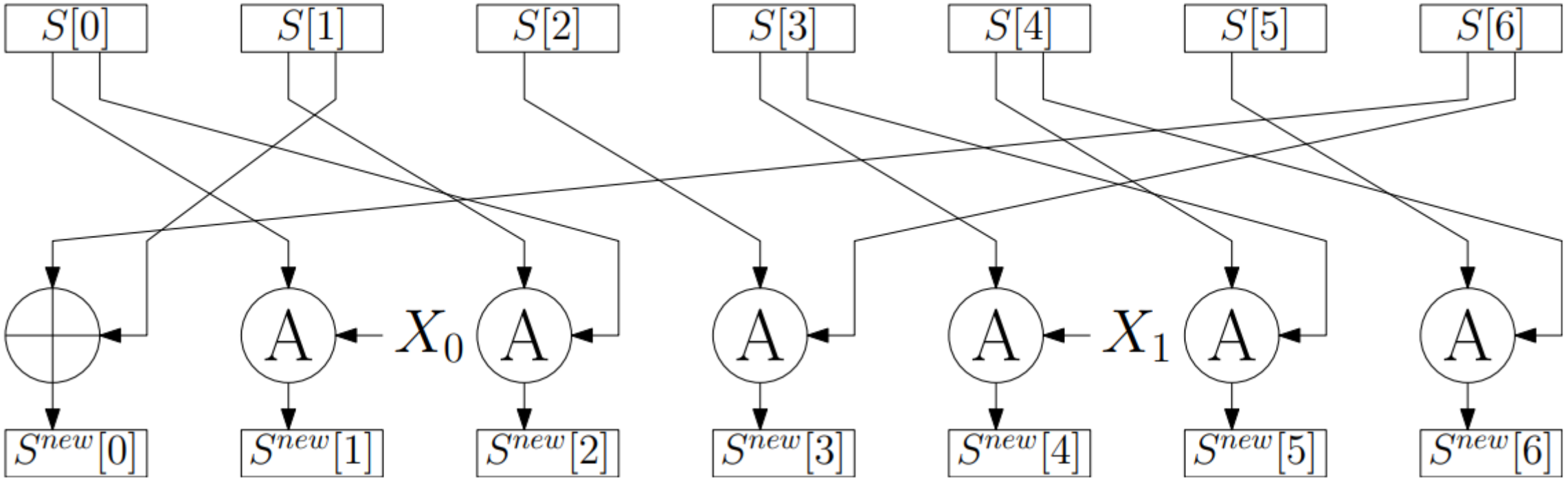
- Increase of throughput:
  - Peak data rate of the Internet is increasing
  - Consideration of new services (e.g. holography, digital twin) requiring higher (100+ Gbps) data rate
- High (256-bit) security encryption algorithm with 100+ Gbps throughput is required

Rocca-S

- Design
  - Sponge-based construction
  - 256-bit key and 256-bit tag
  - three modes: AEAD, encryption only and keystream generation
- Security (in the nonce respecting setting)
  - 256-bit security against key-recovery and forgery attacks
- Performance
  - First algorithm to exceed 200Gbps in software environment
    - 230Gbps (0.122 cycles/bytes) in an encryption only mode
    - 205Gbps in an AEAD mode

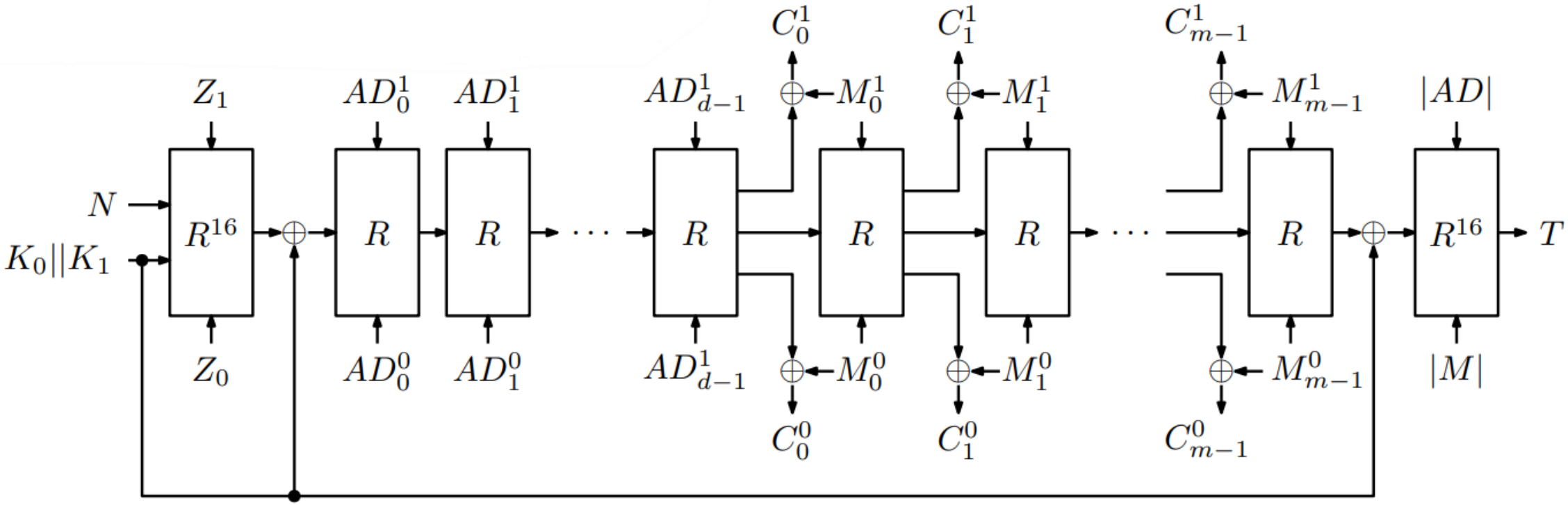
Design: Round function

- Seven 128-bit blocks are updated as $S^{new} = R(S, X_0, X_1)$ with AES round function A and XOR $\oplus$



Design: Procedure

- Four phases: initialization, processing associated data, encryption and finalization



Design: Modes

- Rocca-S supports three modes:
  - AEAD mode
    - encryption + message authentication for plaintext and associated data
  - Encryption only mode
    - Message input to the internal state
    - Decryption will fail with a single bit error
  - Keystream generation mode
    - No message input to the internal state
    - Plaintext can be recovered even when ciphertext bits are flipped, except those flipped ones

Security claim

- 256-bit security against following attacks in the nonce-respecting setting:
  - key-recovery attacks
  - forgery attacks

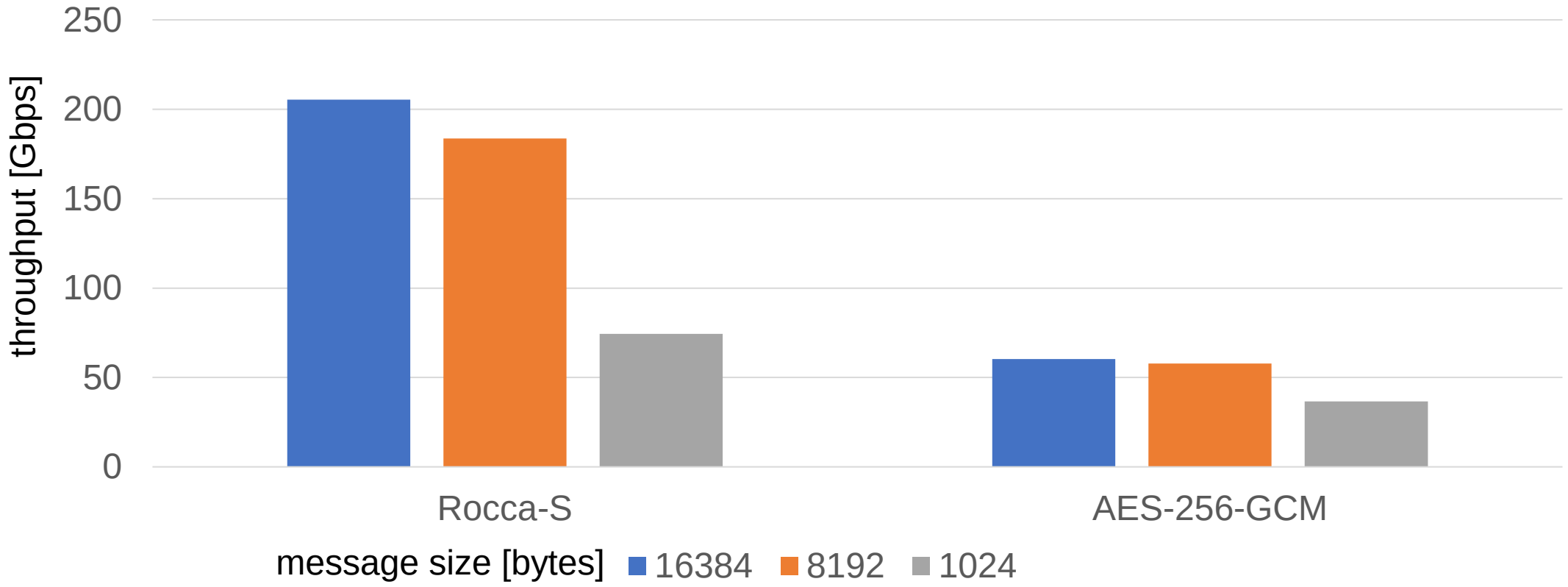
- The lower bound of the number of active S-box (AS) in the initialization phase in single key setting

Rounds	1R	2R	3R	4R	5R	6R	7R	8R	9R	10R	11R	12R
Number	2	7	22	40	**68**	94	113	122	134	152	159	159

- The lower bound of the number of AS is 46 for forgery attack

Performance

- Performance evaluation of AEAD mode with “openssl -speed” on Intel® Core™ i9-12900K



Conclusion

- Encryption algorithm: Rocca-S
  - 256-bit security including forgery
  - 200+ Gbps on PC
  - AEAD, encryption only and keystream generation

- We do not claim any intellectual property rights and restrictions to use
- We plan to provide Rocca-S for OpenSSL on GitHub