AES-based Stream Ciphers

- Paras Dhiman (2021482)
- Rajorshi Mondal (2021187)

SNOW-V Encryption Algorithm

Overview of Snow-V

Introduction:

- A stream cipher developed for 5G systems, derived from SNOW 3G.
- Designed to provide high-speed encryption and robust security.

Applications:

- Mobile network encryption for real-time communication.
- Used in AEAD (Authenticated Encryption with Associated Data) modes.

Performance:

- Achieves speeds of 38 Gbps in AEAD mode.

Architecture of SNOW-V

Linear Feedback Shift Register (LFSR):

- 16-stage register operating over GF(2^8).
- Generates pseudo-random sequences for encryption.

Finite State Machine (FSM):

- Composed of three 32-bit registers.
- Interacts dynamically with LFSR to produce intermediate keystream values.

AES-Inspired Features:

- S-box for non-linear substitution.
- MixColumns transformation for diffusion.

Design Integration:

- Combines the randomness of LFSR with FSM's state transitions.
- Includes AES-like transformations to enhance cryptographic robustness.

Working Mechanism of SNOW-V

Initialization:

- 256-bit key and 128-bit Initialization Vector (IV).
- LFSR and FSM configured to ensure unique encryption states for each session.

Keystream Generation:

- LFSR produces random bit sequences.
- FSM processes these bits to generate the secure keystream.
- S-box and MixColumns operations provide non-linearity and diffusion.

Encryption Process:

- Input plaintext is divided into blocks.
- Keystream is XORed with each plaintext block to produce ciphertext.

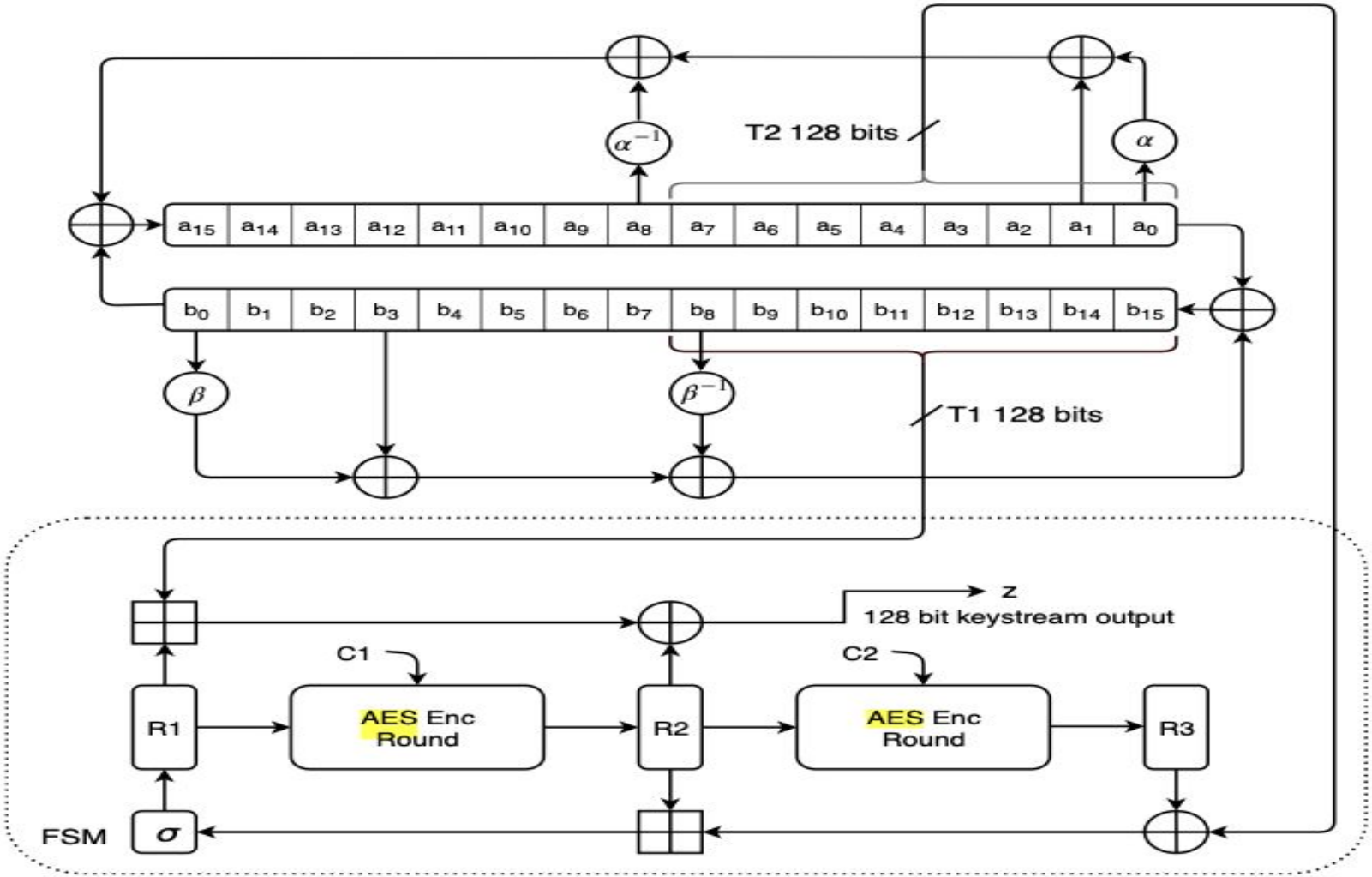
Strengths and Limitations of SNOW-V

Strengths:

- Efficient for hardware and software implementations.
- Robust against linear and differential attacks.
- Low-latency encryption for real-time systems.

Limitations:

- Encryption speed (38 Gbps) insufficient for 6G requirements (>100 Gbps).
- Scaling for high-throughput applications is limited.


T2 128 bits
α^{-1}
α
a_{15} a_{14} a_{13} a_{12} a_{11} a_{10} a_9 a_8 a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0
b_0 b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8 b_9 b_{10} b_{11} b_{12} b_{13} b_{14} b_{15}
β
β^{-1}
T1 128 bits
z
128 bit keystream output
C1
C2
R1
AES Enc Round
R2
AES Enc Round
R3
FSM
σ

Rocca Encryption Algorithm

Overview of Rocca

Introduction:

- AES-based cipher designed for ultra-high-speed environments like 6G.
- Provides both encryption and authentication through AEAD.

Applications:

- Next-generation mobile networks, high-throughput systems, and IoT.

Performance:

- Achieves encryption speeds exceeding 150 Gbps.

Architecture of Rocca

Core Design Principles:

- Feistel Network Structure:
  - Utilizes multiple iterative rounds of substitution, permutation, and mixing.
  - Employs 16-byte block sizes optimized for resource-constrained environments.

AES-Based Primitives:

- Integrates AES operations (SubBytes, ShiftRows, MixColumns, AddRoundKey).
- Designed to align with existing AES hardware accelerations.

Key Scheduling and State Initialization:

- Uses key and nonce values for state configuration.
- Incorporates constants (z0, z1) and a compact state size to ensure efficiency.

Working Mechanism of Rocca

Initialization Phase:

- The 256-bit key and 128-bit nonce initialize the internal state.
- 20 iterations of AES-based round functions ensure secure key mixing.

Associated Data:

- Processes additional metadata securely alongside plaintext.

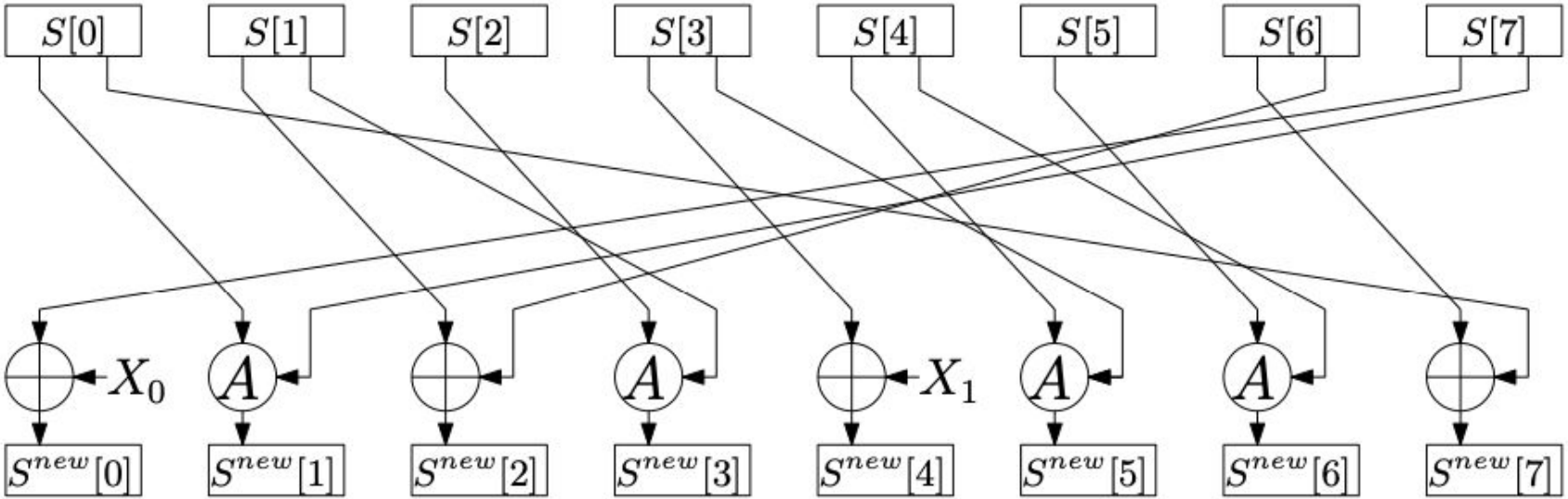
Encryption Phase:

- Processes plaintext through substitution (S-box) and permutation operations.
- Adds round key to current state for block transformations.
- MixColumns provides linear diffusion to enhance security.

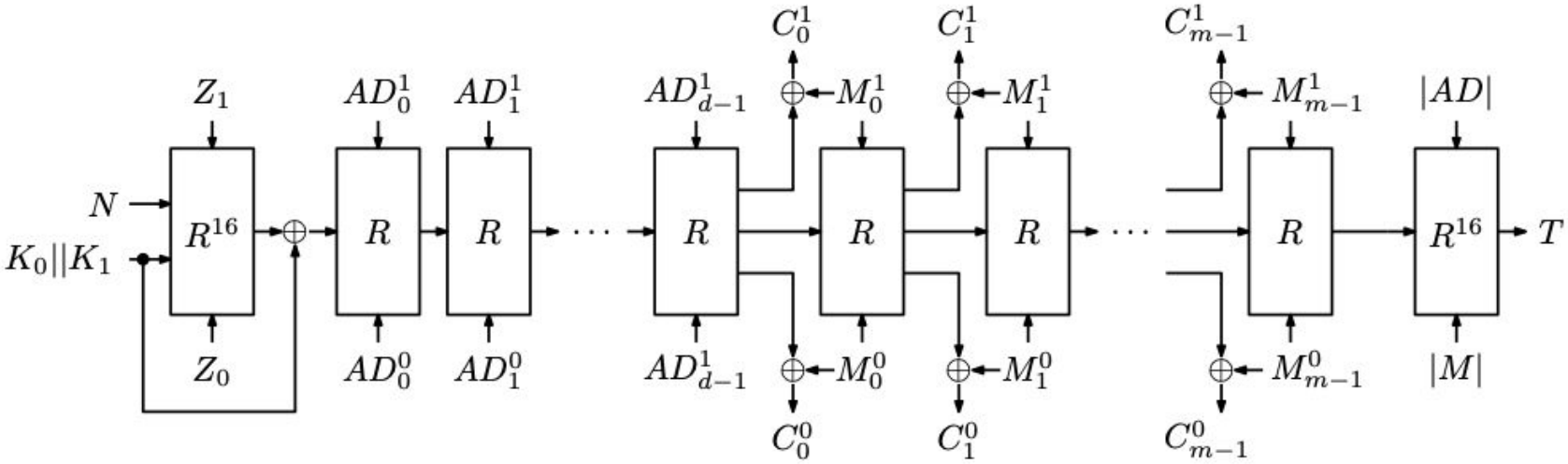
Finalization Phase:

- Generates a 128-bit tag to ensure integrity.

Illustration of Rocca Round Function



Overall Procedure of Rocca



Strengths and Limitations of Rocca

Strengths:

- Exceeds 6G speed requirements with 150 Gbps throughput.
- Robust against forgery and distinguishing attacks.
- Stable performance across varying data sizes.

Limitations:

- More computationally intensive for small plaintext sizes.
- Slightly higher initialization overhead compared to SNOW-V.

Comparison of SNOW-V and Rocca

Performance Metrics

Algorithm	Encryption Speed (Gbps)	Target Use Case
SNOW-V	38	5G real-time applications
Rocca	150	6G high-throughput systems

Encryption Time

Following results were averaged over 100 iterations:

Plaintext Size (bits)	SNOW-V	Rocca
256	0.205 ms	1.36 ms
1024	0.603 ms	1.35 ms
8192	4.20 ms	1.35 ms

Key Differentiators

SNOW-V:

- Excels at low-latency encryption for small data sizes.
- Best suited for real-time 5G systems.

Rocca:

- Scales effectively for large data sizes with stable encryption times.
- Tailored for ultra-high-speed applications in 6G.

Conclusion

Key Insights:

- SNOW-V is a strong candidate for 5G applications requiring low latency.
- Rocca is optimized for 6G systems, with unmatched speed and efficiency.

Practical Recommendations:

- Use SNOW-V for small-scale, latency-sensitive tasks.
- Adopt Rocca for high-speed, large-scale encryption in future networks.