5G Encryption

3GPP/GSMA Cryptographic Algorithms

Algorithms for authentication and key generation:

Cipher	Proprietary	Proprietary	Proprietary	AES	Keccak
Input key size	128	128	128	128	128, 256
Output key size	54	54	64	128	128, 256
Name	COMP-128-1	COMP-128-2	COMP-128-3	MILENAGE	Tuak

Algorithms for encryption and integrity:

Cipher	Proprietary	Proprietary	KASUMI	KASUMI	KASUMI	SNOW 3G	SNOW 3G	AES	AES	ZUC	ZUC
Key size	64	64	64	128	128	128	128	128	128	128	128
Mode	XOR	XOR	f8-mode	f8-mode	CBC-MAC	XOR	CW-MAC1	CTR	CMAC	XOR	CW-MAC2
Type	ENC	ENC	ENC	ENC	INT	ENC	INT	ENC	INT	ENC	INT
2G GSM	A5/1	A5/2	A5/3	A5/4							
2G GPRS	GEA1	GIA2	GEA3	GEA4	GIA4	GEA5	GIA5				
3G UMTS				UEA1	UIA1	UEA2	UIA2				
4G LTE						128-EEA1	128-EIA1	128-EEA2	128-EIA2	128-EEA3	128-EIA3
5G NR						128-NEA1	128-NIA1	128-NEA2	128-NIA2	128-NEA3	128-NIA3

5G Challenges and Requirements

— IMT-2020 (5G) minimum requirements: 20 Gbps (downlink) and 10 Gbps (uplink)

— Network Functions Virtualization (NFV): Software-defined virtualized networks with or without specialized hardware.

	ChaCha20	AES-256-GCM	AES-256-CBC
AMD Ryzen 7 1800X	4.58	21.14	8.81
Intel W-2125	4.52	19.41	9.88
Intel i7-6700	4.68	18.01	9.05

Performance per CPU core in Gbps (https://calomel.org/aesni_ssl_performance.html)

— AES-CMAC has similar performance as AES-CBC in software and SNOW 3G is slightly slower.

— New 256-bit algorithm(s) needed in 5G for performance, government usage, and future proofing.

— Two high performance algorithms are included in the CEASAR final portfolio: AES-OCB3 and AEGIS-128.

SNOW V: A new version of SNOW for 5G

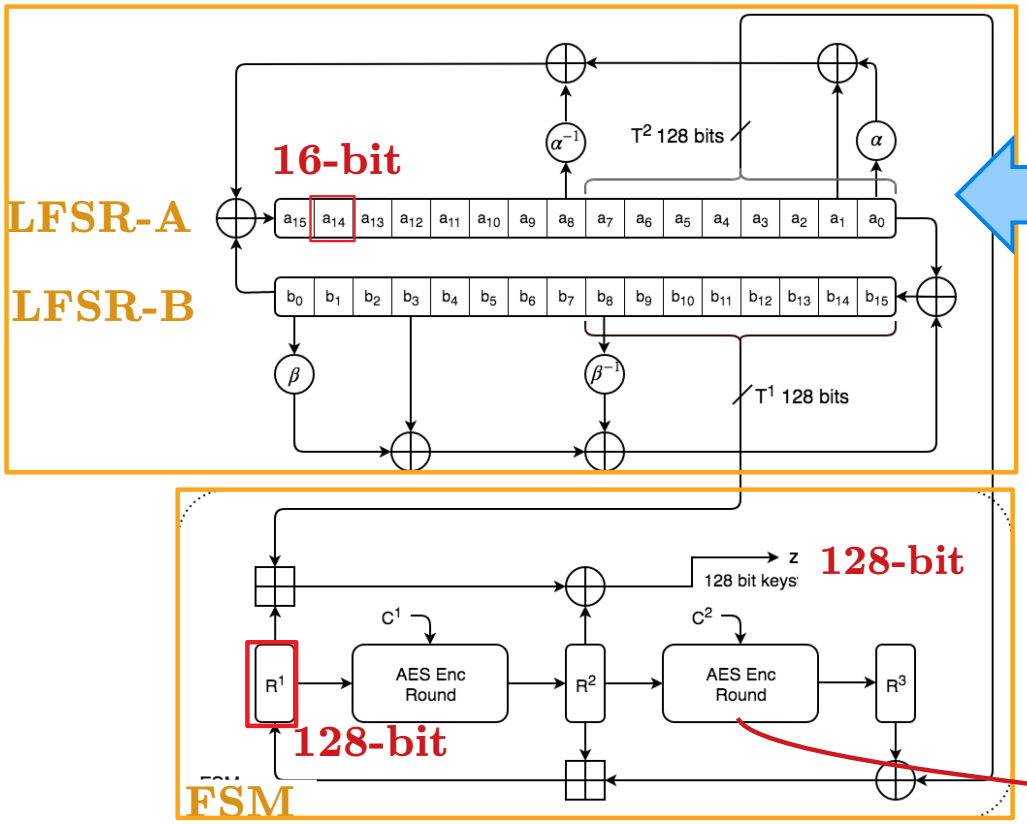
Patrik Ekdahl[2], Thomas Johansson[1], Alexander Maximov[2], Jing Yang[1]

[1] Department of Electrical and Information Technology, Lund University

[2] Ericsson Research, Ericsson

SNOW-V Construction

- A stream cipher designed for modern CPUs (SIMD, AES-NI)
- Builds on the design and trust in previous versions of SNOW



2x 256-bit AVX2 registers

- LFSR: 2x256 bits
- FSM: 3x128-bit registers and 2 AES rounds
- Output: 128-bit keystream

Security goal: not worse than AES-256

AES-NI

	LFSRs	LFSR Stages	Stage Sizes	FSM Register Sizes	Output
SNOW 3G	1	16	32-bit	32-bit	32-bit
SNOW V	2	32	16 -bit	128-bit	128-bit

SNOW-V Performance and Next Steps

- **Performance:**
  - In software, SNOW-V reaches above 60 Gbps on a mainstream laptop CPU (i7-8650U) (single thread).
  - In hardware, SNOW-V reaches above 700 Gbps and are expected to reach 1000 Gbps on 7 mm ASIC.
- **Next steps:**
  - More security analysis, especially from independent cryptanalysts.
  - More performance measurements on server-grade ARM (e.g. Cortex-A72), 7 mm ASIC, etc.
  - SNOW-V paper uses GCM/GHASH for integrity protection. Will evaluate other faster options.
  - 3GPP SA3 has given requirements to ETSI SAGE, ETSI SAGE will recommend algorithm(s) to 3GPP SA3.
- **Conclusions:**
  - Opportunities to do more efficient encryption by designing algorithms for modern CPUs.