A Telco Security Christmas List

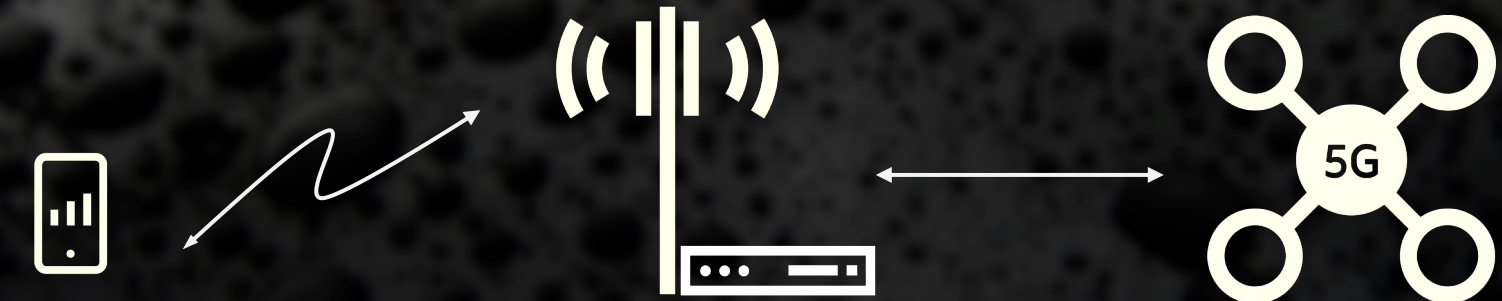
Patrik Ekdahl
Head of Platform Security Research
Ericsson Research

Short Introduction

- M.Sc.EE, Lund University 1998
- Ph.D. in Cryptology, Lund University 2003
- Building crypto equipment for Swedish Defence 2004-2007
- Ericsson Research 2007-
  - Crypto algorithms
  - Standardisation work (TCG, GlobalPlatform)
  - Trusted Environments, HW Security
  - Head of Platform Security Research since 2014
- Chair of ETSI/SAGE since 2021

- Plays the trumpet (big band jazz)
- Enjoys wood, metal and leather crafts

The holy trinity of the 3GPP telco system

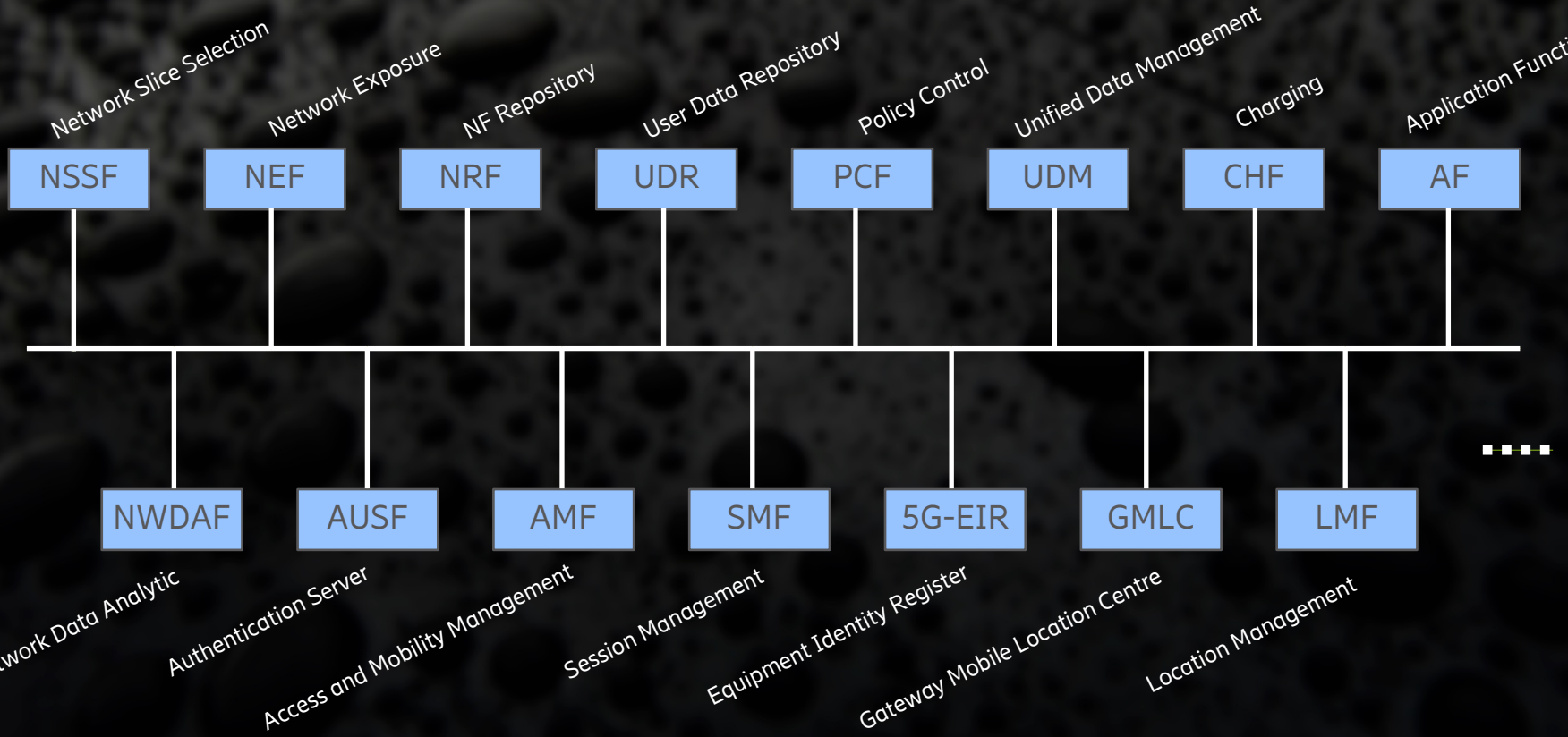


Device

Radio Access Network

Core Network

Network Functions (NFs) of the 5G Core



What comprises a NF?

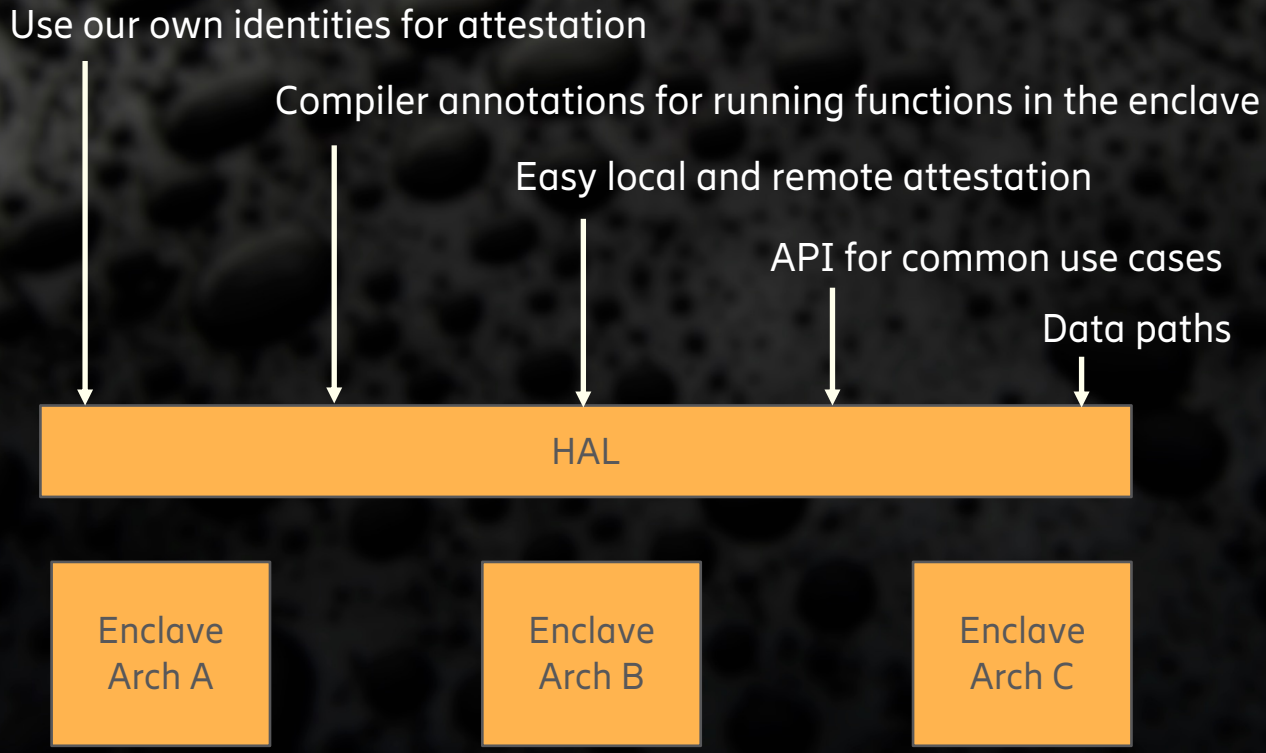
The microservices of the Session Management Function (SMF):

A 5G Core example deployment

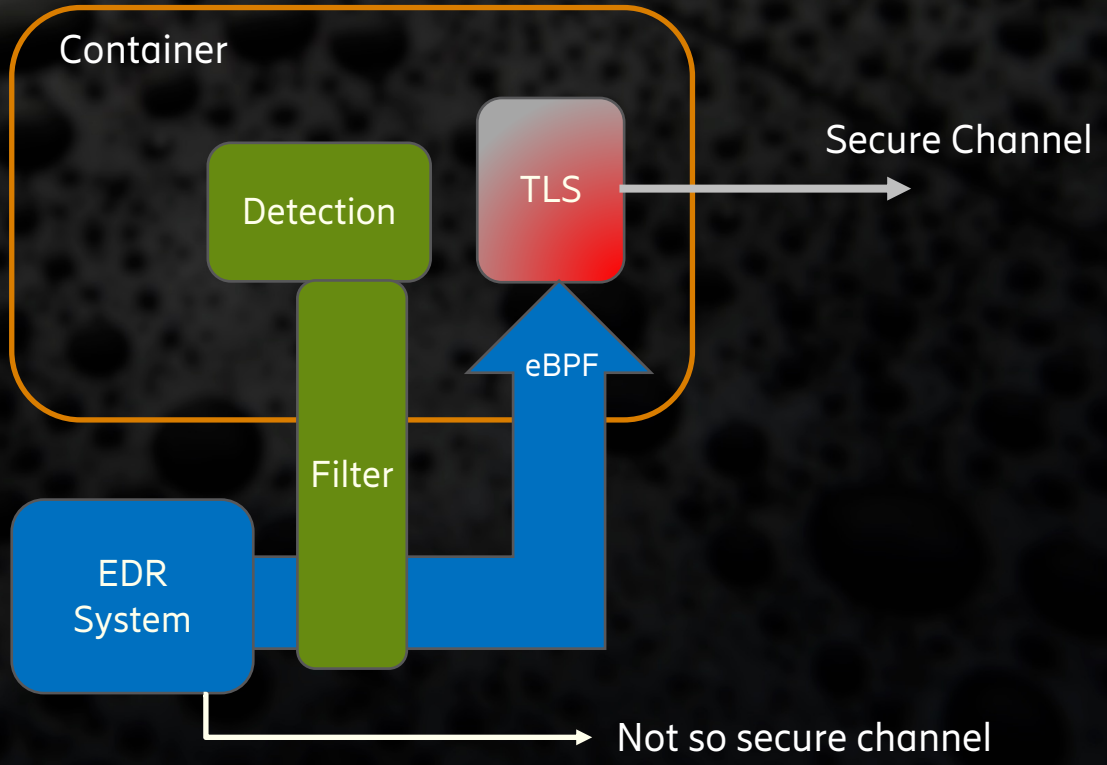
- 4 million users in AMF
- 4 million sessions in SMF

Roughly
- 650 microservices
- 20 servers
- 70 enclaves per server

HAL for enclaves

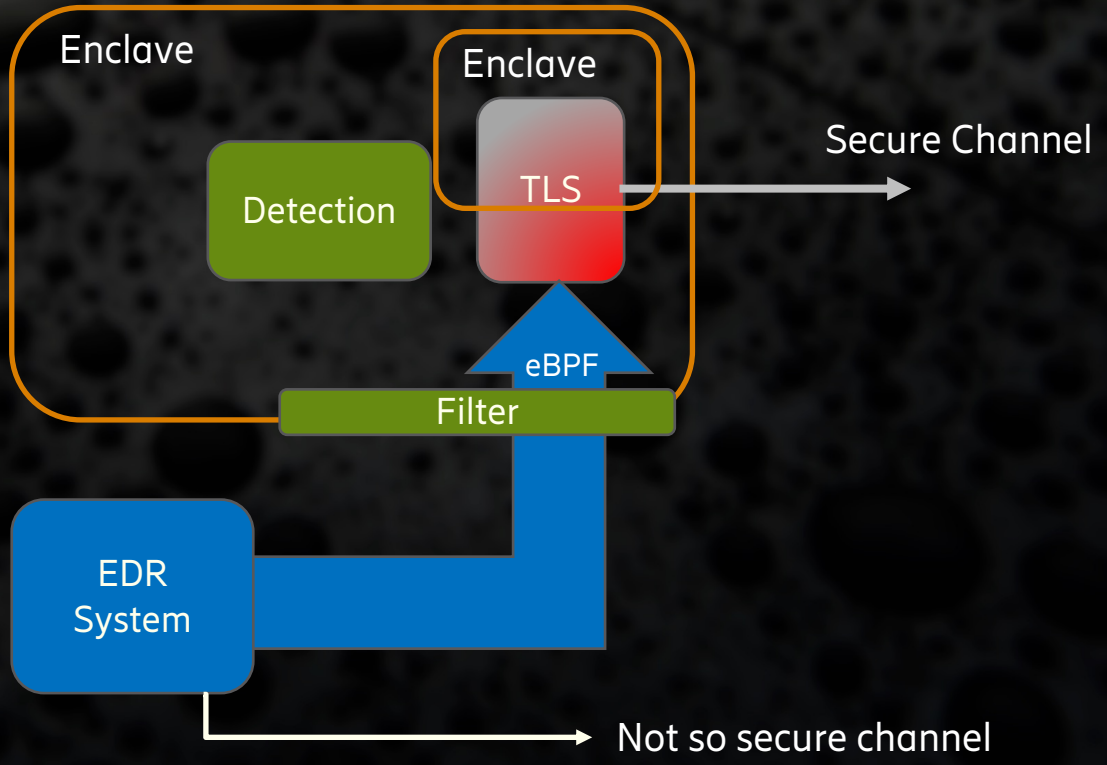


Nested Enclaves with Transparent Endpoint Detection & Response (EDR)

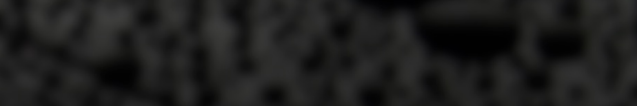


Nested Enclaves with Transparent Endpoint Detection & Response (EDR)

- Nested enclaves with different accessibility and security levels.
- Reliably choose what the EDR system can see inside an enclave.
- Side-channel protection for enclaves.
  - SW/HW responsibilities?

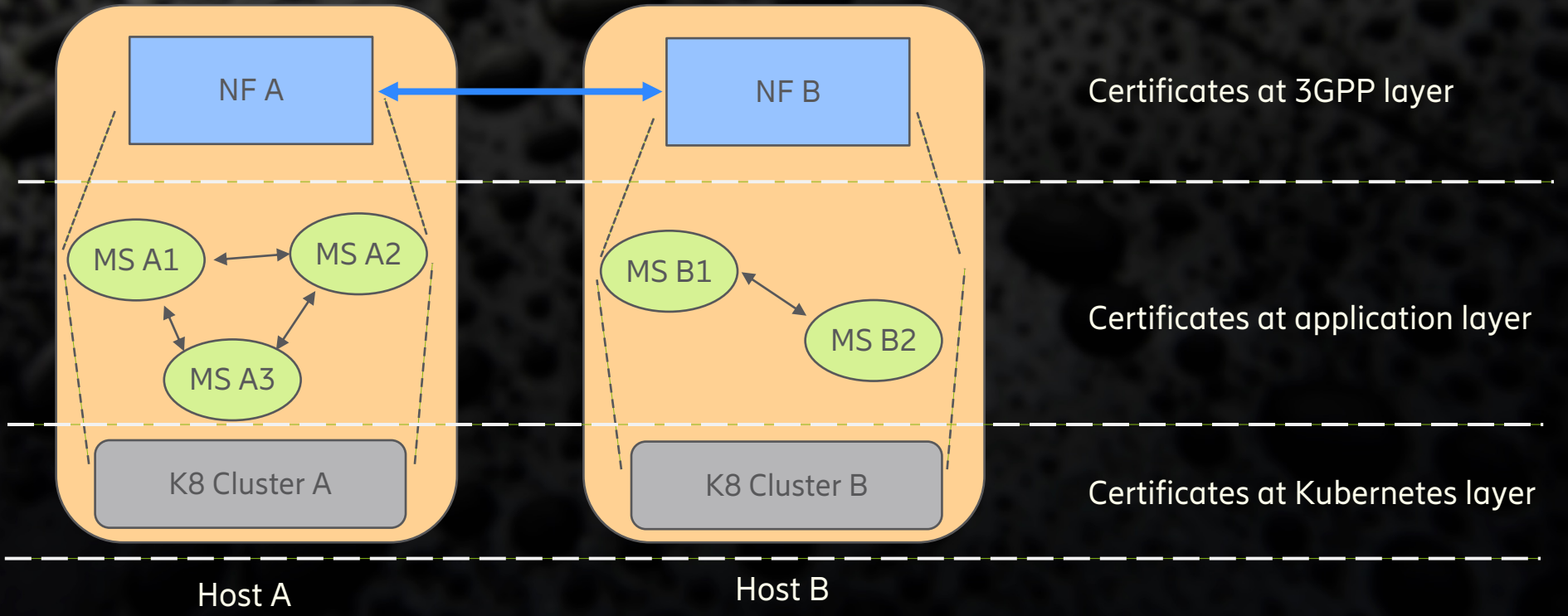


Enclaves for FPGAs

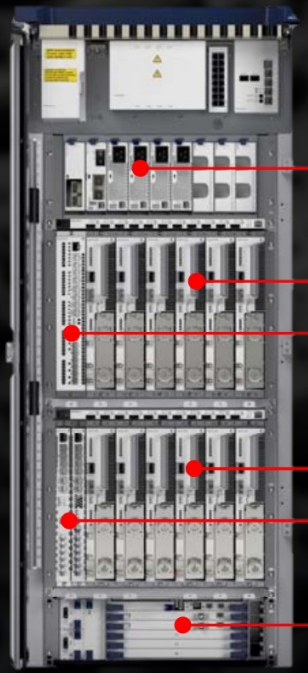


- Dynamically reprogram the FPGA with confidential bitstreams
- How to manage trust?
- Bitstream inspection needed?
- Can the manufacturer take responsibility for protection agains the hardware owner?
- What would be needed to enable secure multi-tenancy?

The Certificate Nightmare



Radio Basestation



Site Power

Radio Units

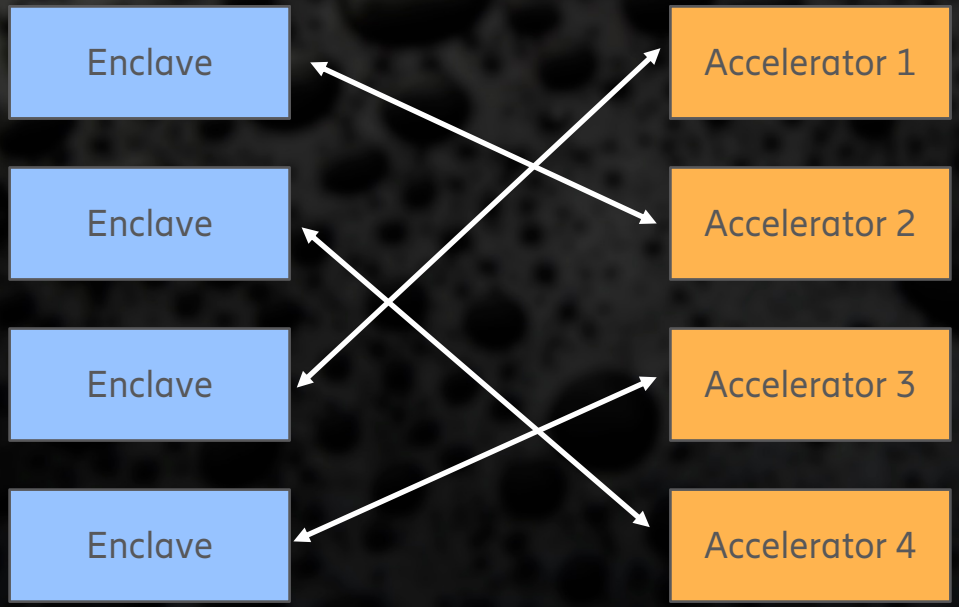
Digital Unit

Radio Units

Digital Unit

Transmission

Accelerators and Enclaves



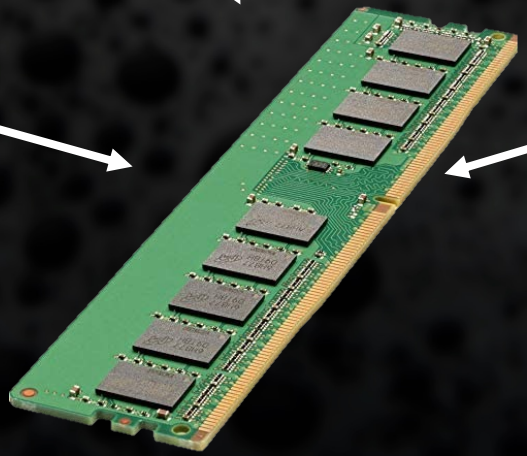
Extend the enclave story to peripherals.

SDRAM integrity

Random errors

Software attacks

Physical attacks



Interchip communication CI(A)

Confidentiality and Integrity

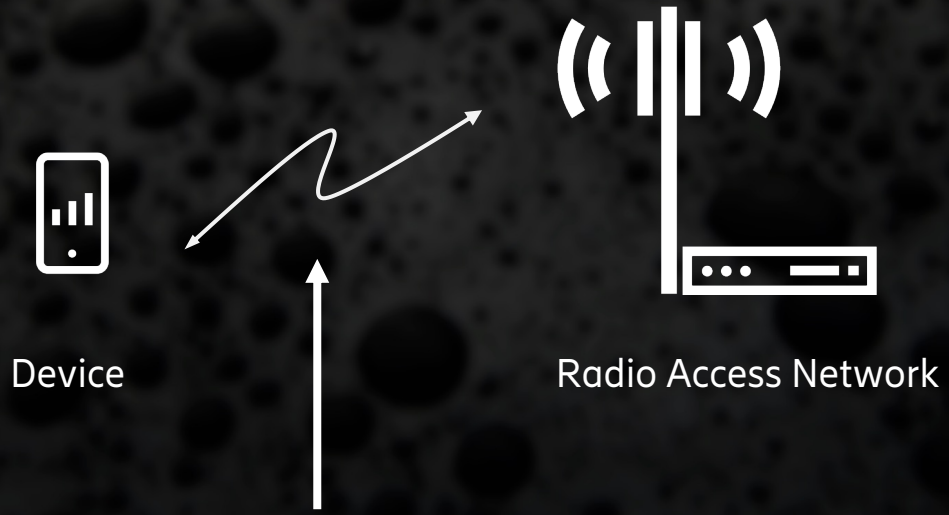
Three types:
- Slow, easy to attack interfaces (i2c, spi etc)
- Parallel high speed interfaces (mainly SDRAM DDRx)
- Serial high speed interfaces (Ethernet, CXL, PCIe)

Lightweight
- Power
- Performance
- Latency

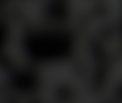
Physical Attack Mitigation

New 256-bit algorithms for 3GPP air interface

Specifications written by ETSI SAGE was finished in November



Requirements



- 256 bit key size
- Handle 20Gbs encryption speeds
- Virtualisation friendly on a variety of CPU architectures
- Longer MACs (currently 32 bit tags are used)

History

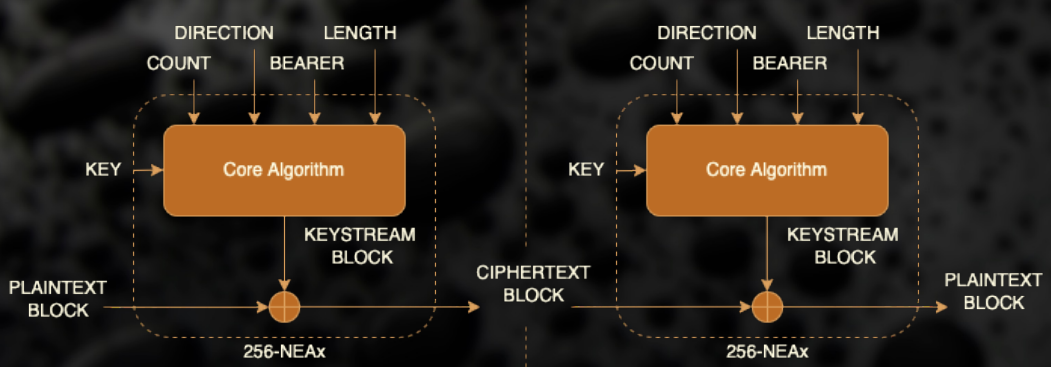
Base algorithm	3G	4G	5G 128 bits
Kasumi	UxA1		
Snow 3G	UxA2	128-ExA1	128-NxA1
AES-128		128-ExA2	128-NxA2
ZUC-128		128-ExA3	128-NxA3

x = E for Encryption
x = I for Integrity

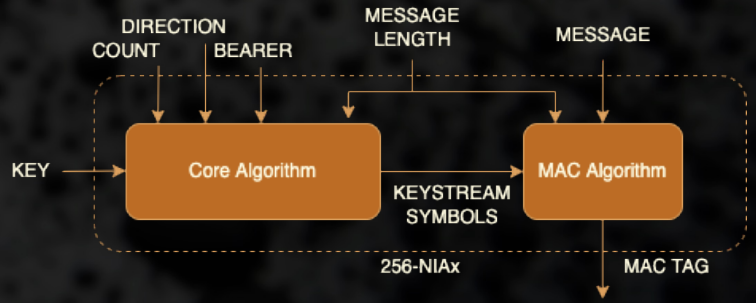
Nine 256-bit algorithms

	Snow 5G	AES-256 (CTR)	ZUC-256
Confidentiality	256-NEA1	256-NEA2	256-NEA3
Integrity	256-NIA1	256-NIA2	256-NIA3
Authenticated Encryption with Additional Data (AEAD)	256-NCA1	256-NCA2	256-NCA3

Overview of the traditional modes



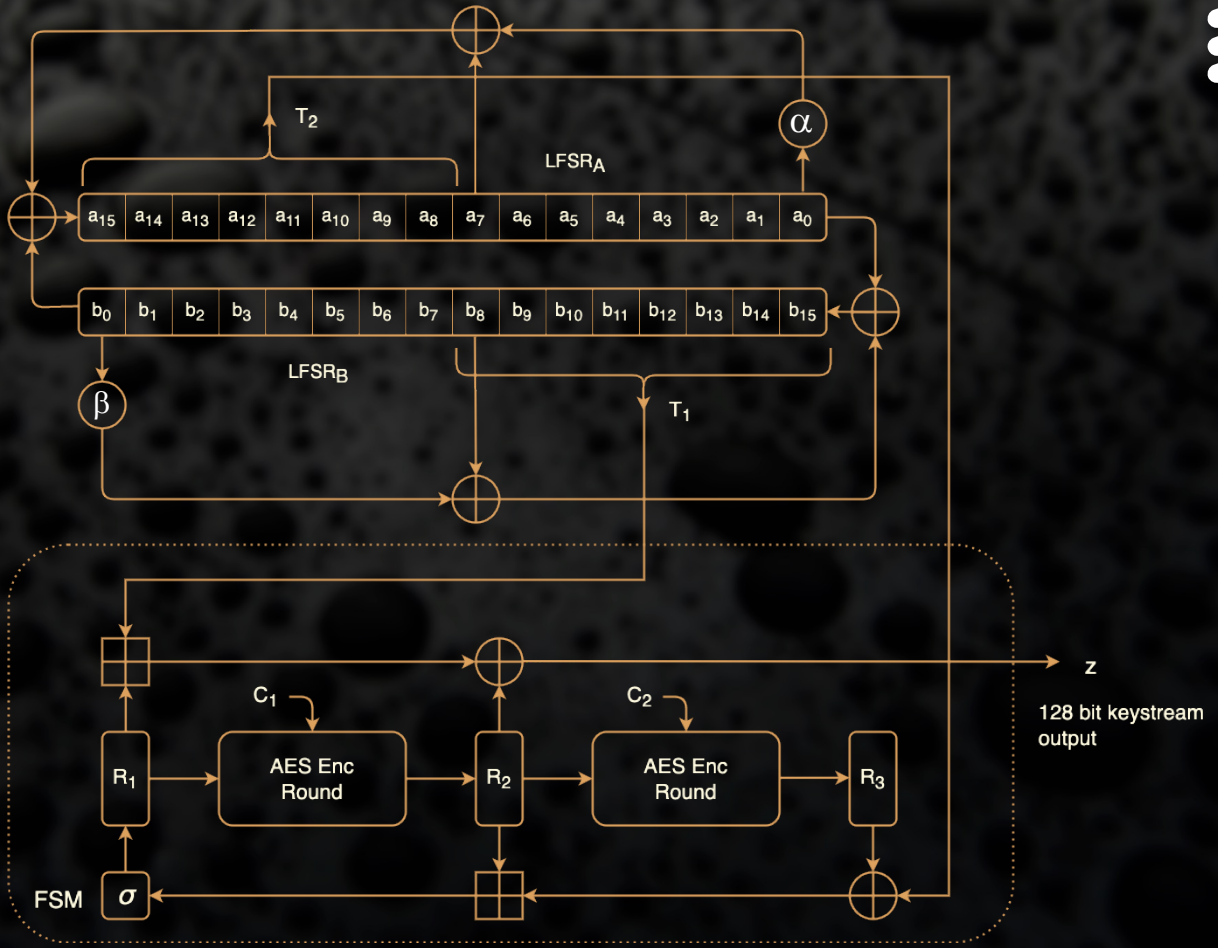
Overview of the 256-NEAx algorithm encryption and decryption



Overview of the 256-NIAx algorithm MAC generation.

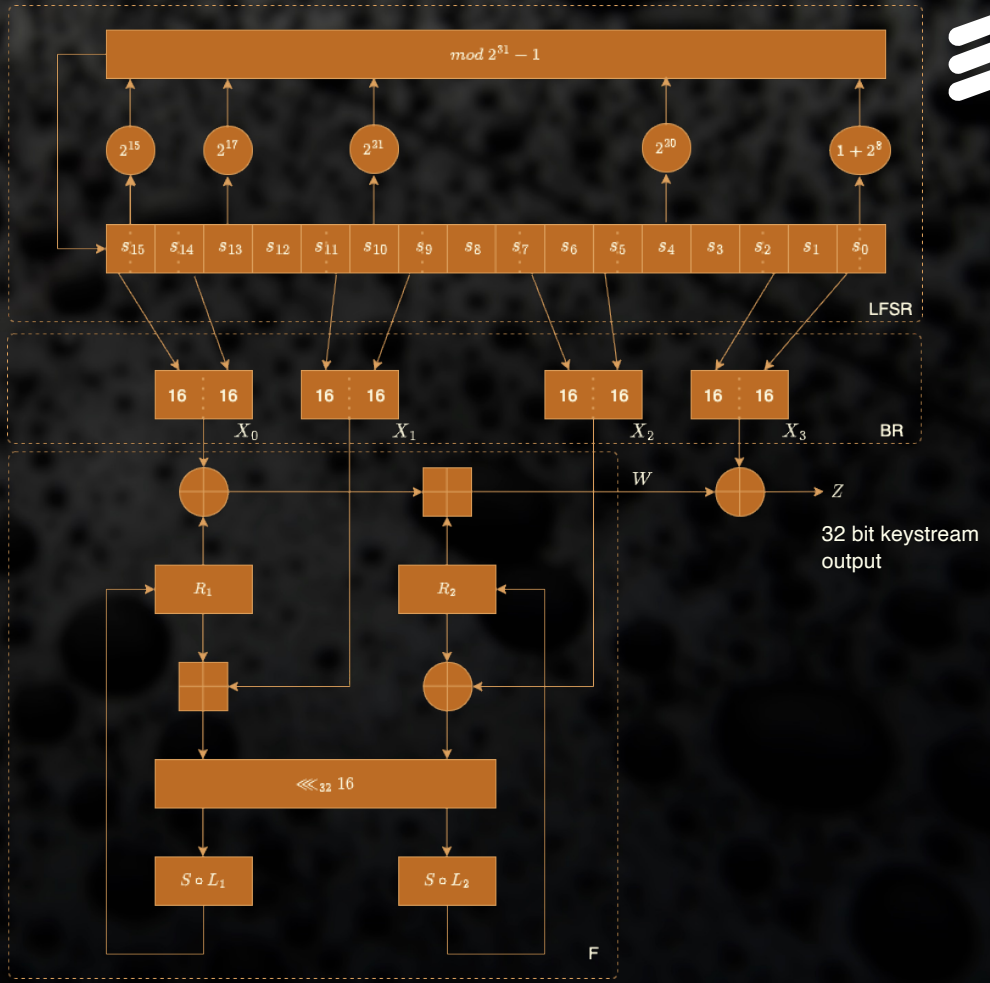
Tag sizes are from 4...16 bytes.
(4 previous)

SNOW-Vi


T2
α
LFSRA
a15 a14 a13 a12 a11 a10 a9 a8 a7 a6 a5 a4 a3 a2 a1 a0
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
LFSRB
β
T1
C1
C2
R1
AES Enc Round
R2
AES Enc Round
R3
FSM
σ
z
128 bit keystream output

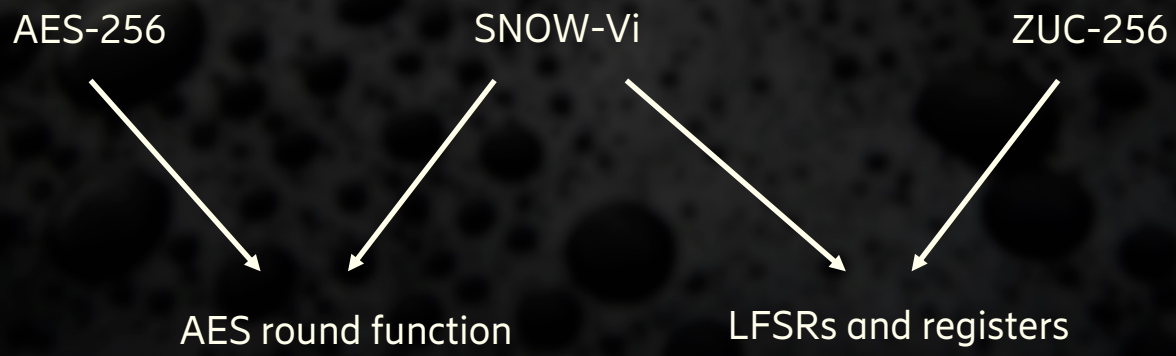
ZUC-256

- Exactly the same layout as ZUC-128.
- New initialisation (Key, IV)
- SAGE recommends 48(+1) initialisation rounds instead of 32(+1)



Master Thesis proposal

Make a combined hardware implementation of these core algorithms, reusing as much as possible.



In the Snow-V paper, there is a 64 bit pipelined implementation that only uses 1 AES round function.

ERICSSON