



ÚRAD PODPREDESEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

<> CSIRT.SK

Mobilné siete

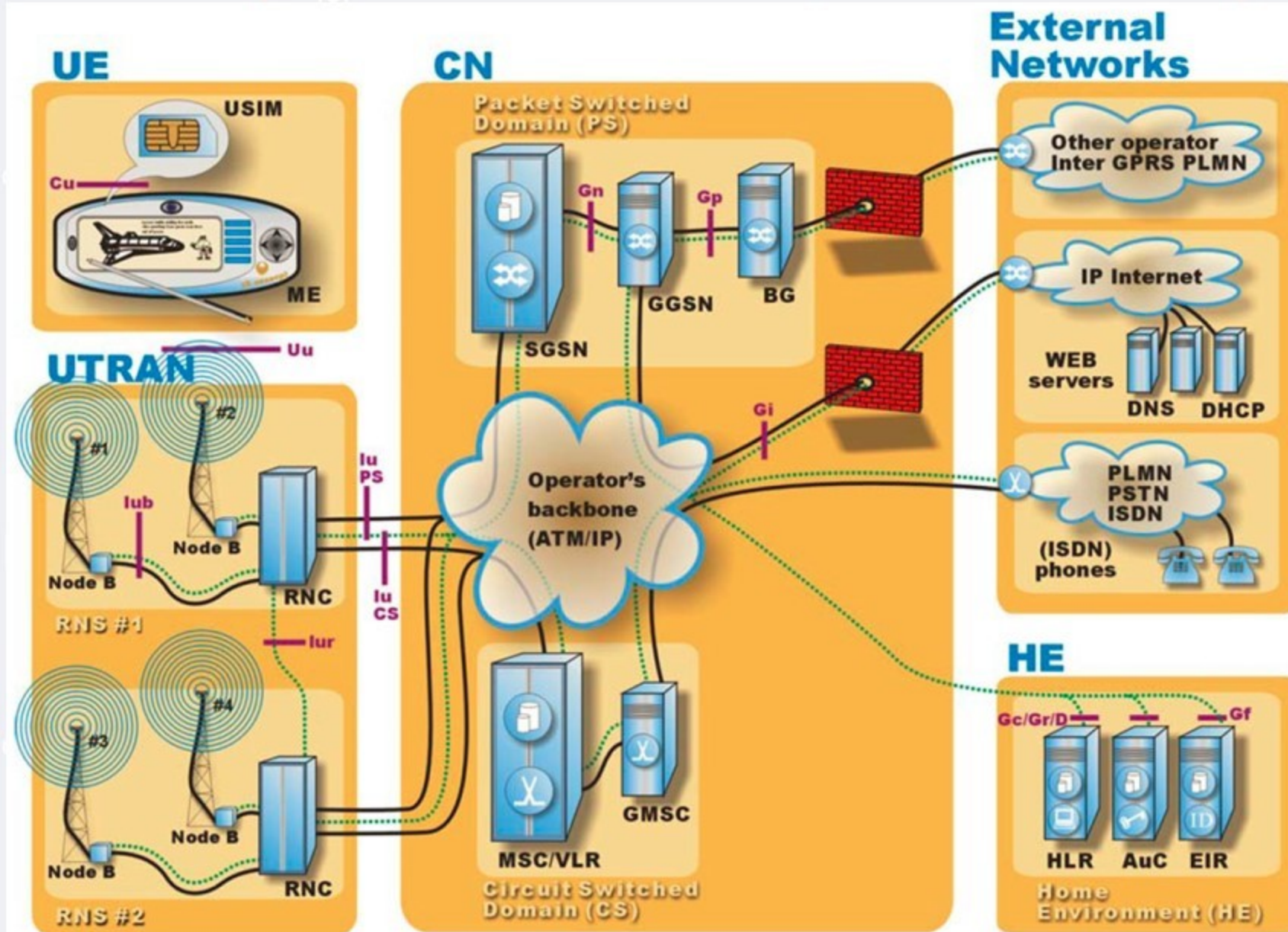
CSIRT.SK

Kľúčové slová

- Ki
- Kc
- RAND
- SRES (XRES)
- RES
- A3, A5
- IMSI – 15 čísel
- AUTN, MAC, SQN

Kľúčové slová

- USIM - Universal Subscriber Identity Module
- UE - User Equipment
- SRNC - Serving Radio Network Controller
- VLR - Visitor Location Register
- SQN - Sequence number
- AuC - Authentication Centre
- AUTN | S - Authentication token | Synchronization



GSM autentifikácia

MS/USIM/UE

RNC
BTS/VLR/SRNC

AuC



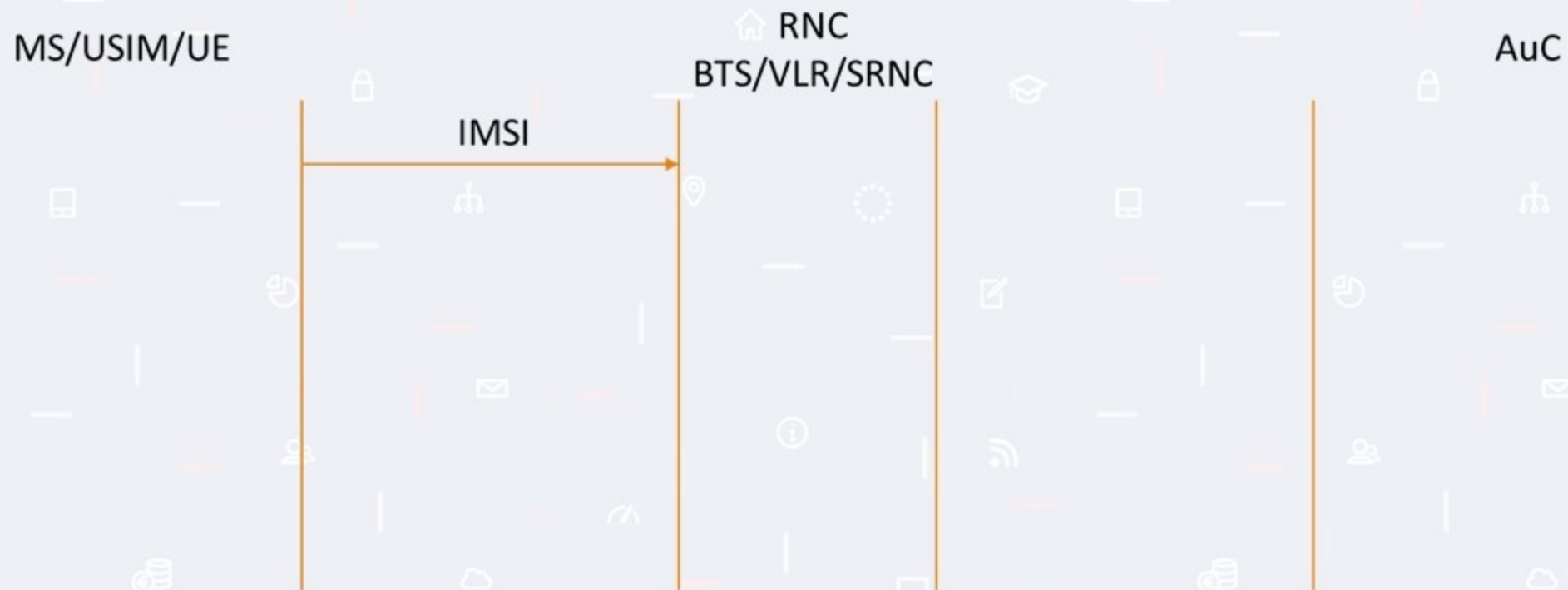
ÚRAD PODPREDESEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

 CSIRT.SK

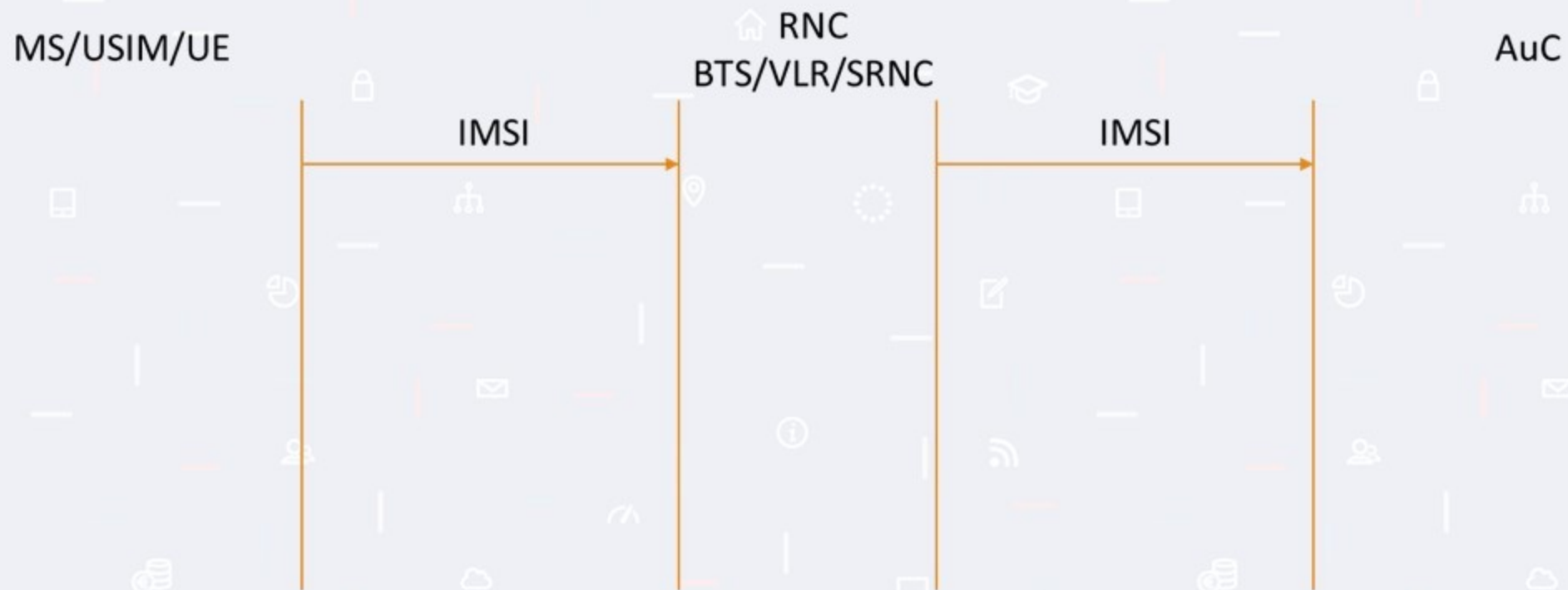
+421 2 59 278 262
info@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

GSM autentifikácia



GSM autentifikácia



GSM autentifikácia

MS/USIM/UE

RNC
BTS/VLR/SRNC

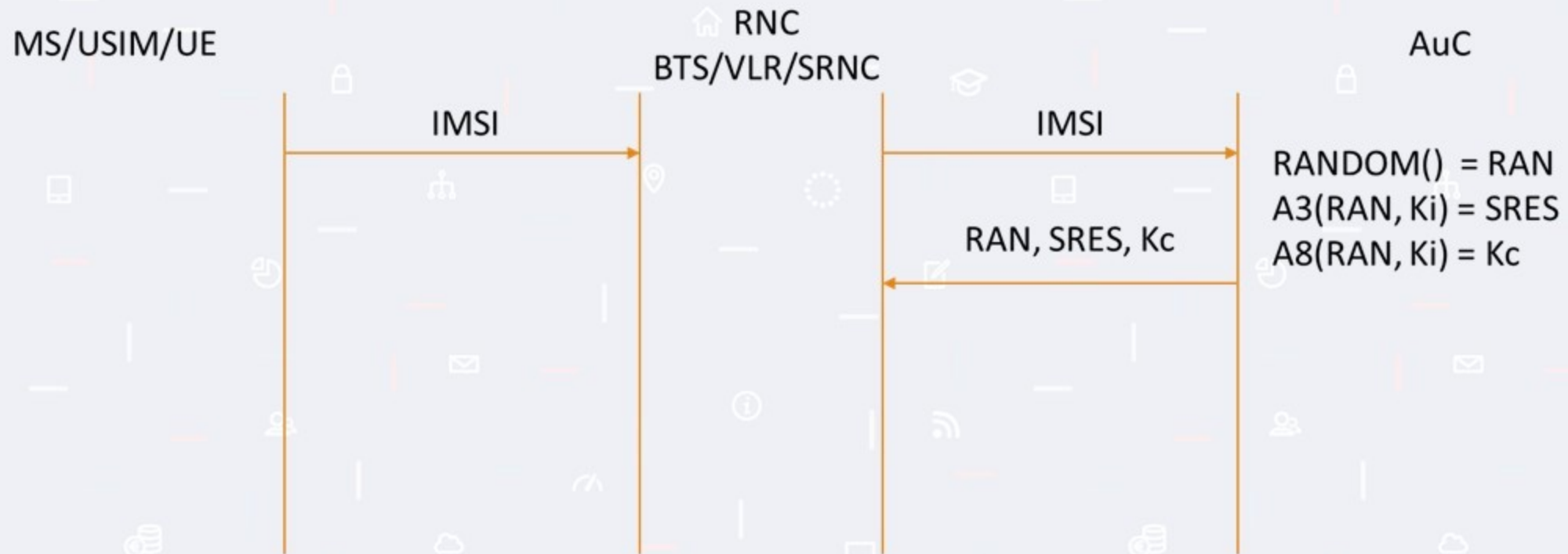
AuC

IMSI

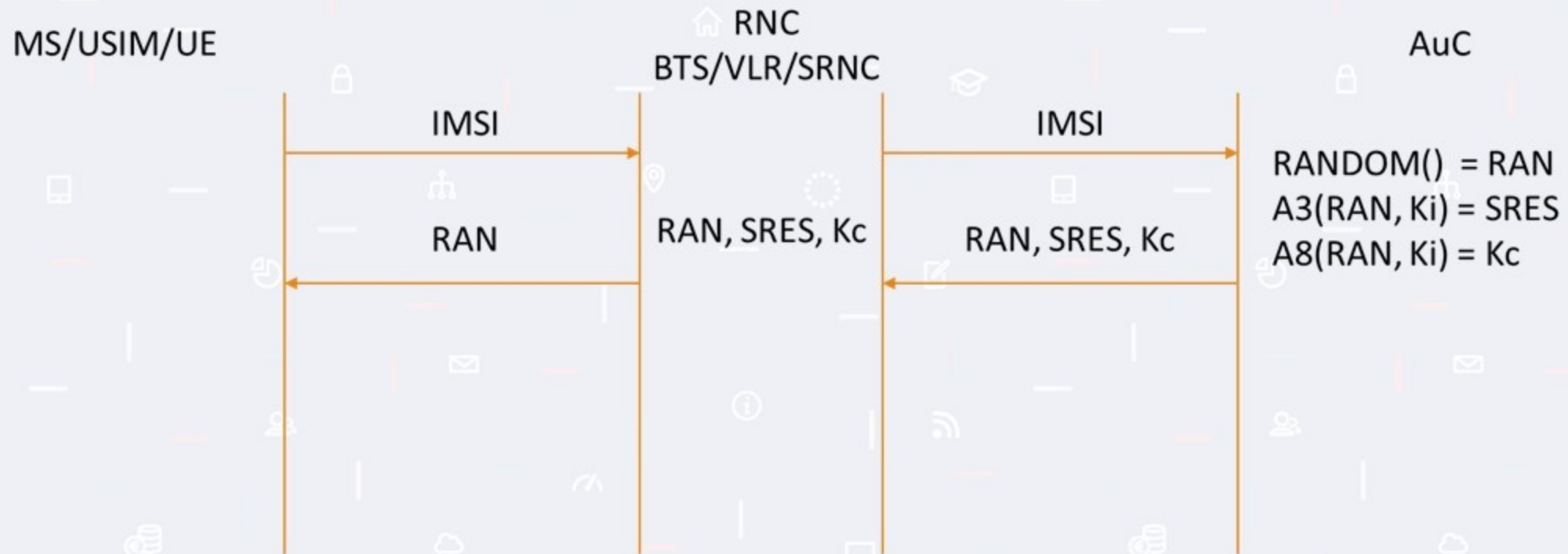
IMSI

$\text{RANDOM}() = \text{RAN}$
 $\text{A3}(\text{RAN}, \text{Ki}) = \text{SRES}$
 $\text{A8}(\text{RAN}, \text{Ki}) = \text{Kc}$

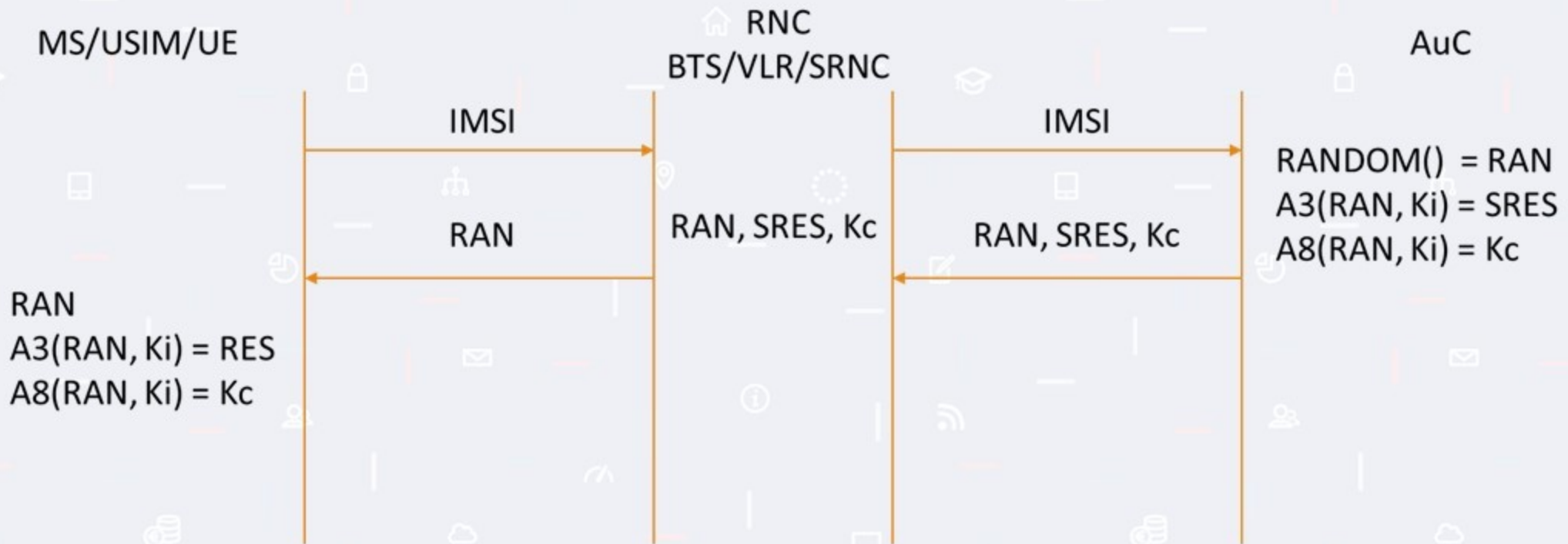
GSM autentifikácia



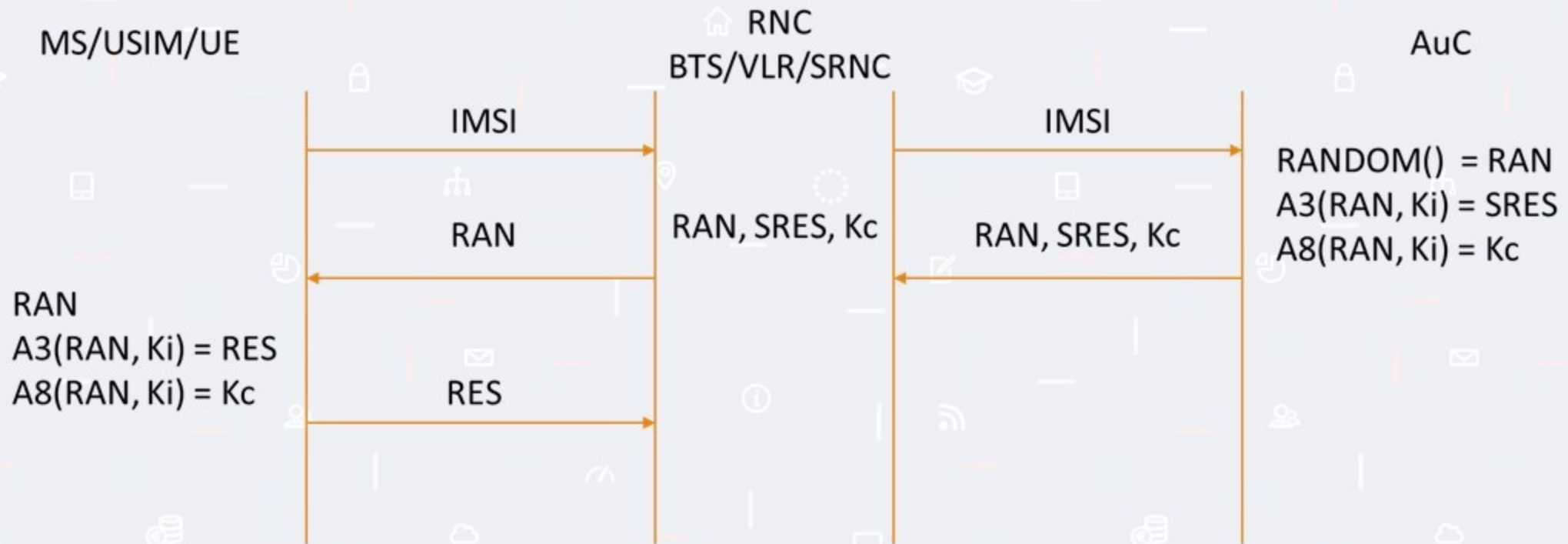
GSM autentifikácia



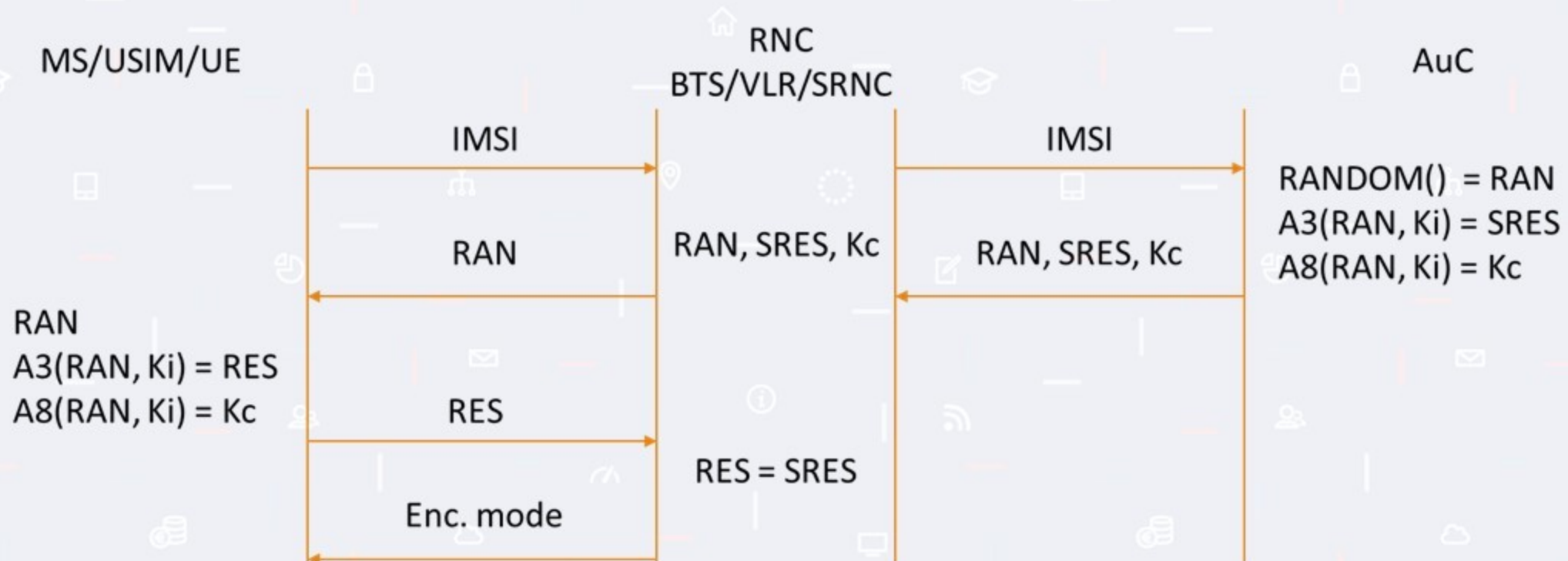
GSM autentifikácia



GSM autentifikácia



GSM autentifikácia



História chýb algoritmov

- 1991 – GSM implementácia
- Apríl 1998 - The Smartcard Developer Association (SDA) spolu s U.C. Berkeley researchers prelomili COMP128 algoritmus uložený v SIM karte a úspešne získali Ki v priebehu pár hodín. Zistili, že Kc používa iba 54 bitov.
- August 1999: Slabá A5/2 bola prelomená použitím PC v priebehu pár sekúnd.
- December 1999: Alex Biryukov, Adi Shamir a David Wagner publikovali schému útoku na algoritmus A5/1. Pri získaní dvoch minút rozhovoru boli schopný prelomiť A5/1 algoritmus v priebehu 1 sekundy.
- Máj 2002: IBM Research group objavila nový spôsob rýchleho získavania Kc z COMP128 použitím útokov side channels.

3G a LTE

Funkcia	Popis	Výstup	Lokácia	Status	Bit
f0	Náhodné čísla	RAN	AuC	Op. špec.	128
f1	Sieťová autentifikácia	(X)MAC-A	USIM, AuC	Op. Špec., (M)	64
f1*	Sieťová autentifikácia resynch.	(X)MAC-S	USIM, AuC	Op. Špec., (M)	64
f2	Užívateľská autentifikácia	RES/XRES	USIM, AuC	Op. Špec., (M)	32-128
f3	Derivácia kľúča pre šifru	CK	USIM, AuC	Op. Špec., (M)	128
f4	Derivácia kľúča pre integritu	IK	USIM, AuC	Op. Špec., (M)	128
f5	Derivácia kľúča pre anonymitu	AK	USIM, AuC	Op. Špec., (M)	48
f5*	Derivácia kľúča pre anonymitu resynch.	AK	USIM, AuC	Op. Špec., (M)	48
f8	Šifrovacia funkcia	...	MS, RNC	PŠ(K,S,AES)	
f9	Generovanie pečiatky integrity	MAC-I/XMAC-I	MS, RNC	PŠ(K,S,AES)	32
K	Kľúč na karte – zdieľaný	Žiadny	USIM, AuC		128

3G a LTE

MS/USIM/UE

RNC
BTS/VLR/SRNC

AuC



ÚRAD PODPREDESEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

 **CSIRT.SK**

+421 2 59 278 262
info@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

3G a LTE

MS/USIM/UE

RNC
BTS/VLR/SRNC

AuC

IMSI

```
sequenceDiagram
    participant MS as MS/USIM/UE
    participant RNC as RNC  
BTS/VLR/SRNC
    participant AuC as AuC
    MS->>RNC: IMSI
```

The diagram illustrates a sequence of interactions between three entities: MS/USIM/UE, RNC/BTS/VLR/SRNC, and AuC. Three vertical orange lines represent the lifelines of these entities. An orange arrow labeled 'IMSI' points from the MS/USIM/UE lifeline to the RNC/BTS/VLR/SRNC lifeline. The AuC lifeline is present but has no messages associated with it in this specific sequence.



3G a LTE

MS/USIM/UE

RNC
BTS/VLR/SRNC

AuC

IMSI

IMSI



3G a LTE

MS/USIM/UE

RNC
BTS/VLR/SRNC

AuC

IMSI

IMSI

$\text{RANDOM}() = \text{RAN}$
 $\text{AV}(\text{IMSI}, \text{RAN}) = \text{AV}(1, \dots, n)$
 $\text{AV}(1, \dots, n) = \text{XRES} || \text{CK} || \text{IK} ||$
 $|| \text{AUTN} || \text{RAN}$

$\text{AUTN} = \text{SQN} \text{ xor } \text{AK} || \text{AMF} ||$
 $|| \text{MAC}$



3G a LTE

MS/USIM/UE

RNC
BTS/VLR/SRNC

AuC

IMSI

IMSI

AV(1,...,n)

$\text{RANDOM}() = \text{RAN}$
 $\text{AV}(\text{IMSI}, \text{RAN}) = \text{AV}(1, \dots, n)$
 $\text{AV}(1, \dots, n) = \text{XRES} || \text{CK} || \text{IK} ||$
 $|| \text{AUTN} || \text{RAN}$

$\text{AUTN} = \text{SQN} \text{ xor } \text{AK} || \text{AMF} ||$
 $|| \text{MAC}$



3G a LTE

MS/USIM/UE

RNC
BTS/VLR/SRNC

AuC

IMSI

IMSI

RAN || AUTN

XRES, CK, IK
AUTN, RAN

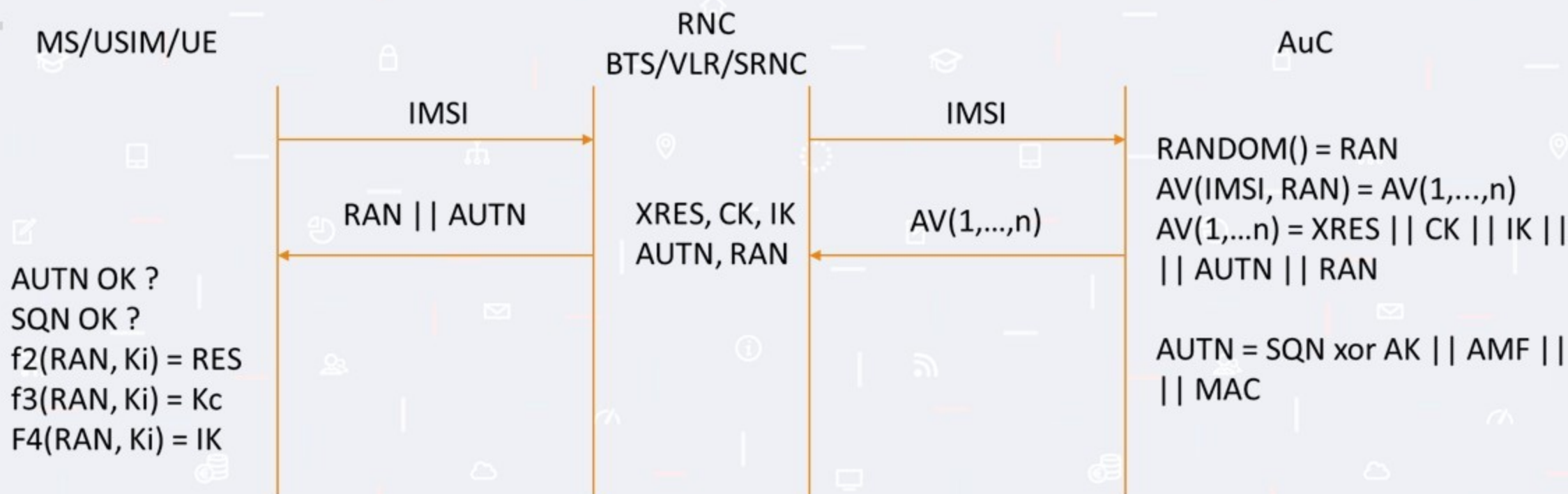
AV(1,...,n)

$\text{RANDOM}() = \text{RAN}$
 $\text{AV}(\text{IMSI}, \text{RAN}) = \text{AV}(1, \dots, n)$
 $\text{AV}(1, \dots, n) = \text{XRES} || \text{CK} || \text{IK} ||$
 $|| \text{AUTN} || \text{RAN}$

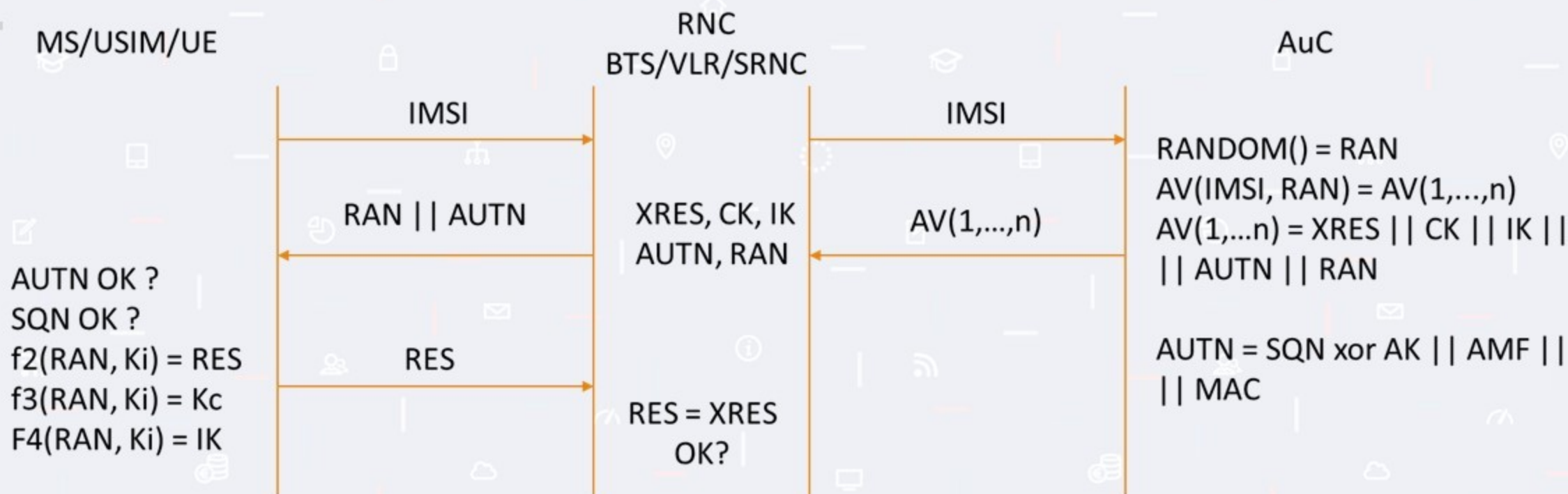
$\text{AUTN} = \text{SQN} \text{ xor } \text{AK} || \text{AMF} ||$
 $|| \text{MAC}$



3G a LTE



3G a LTE



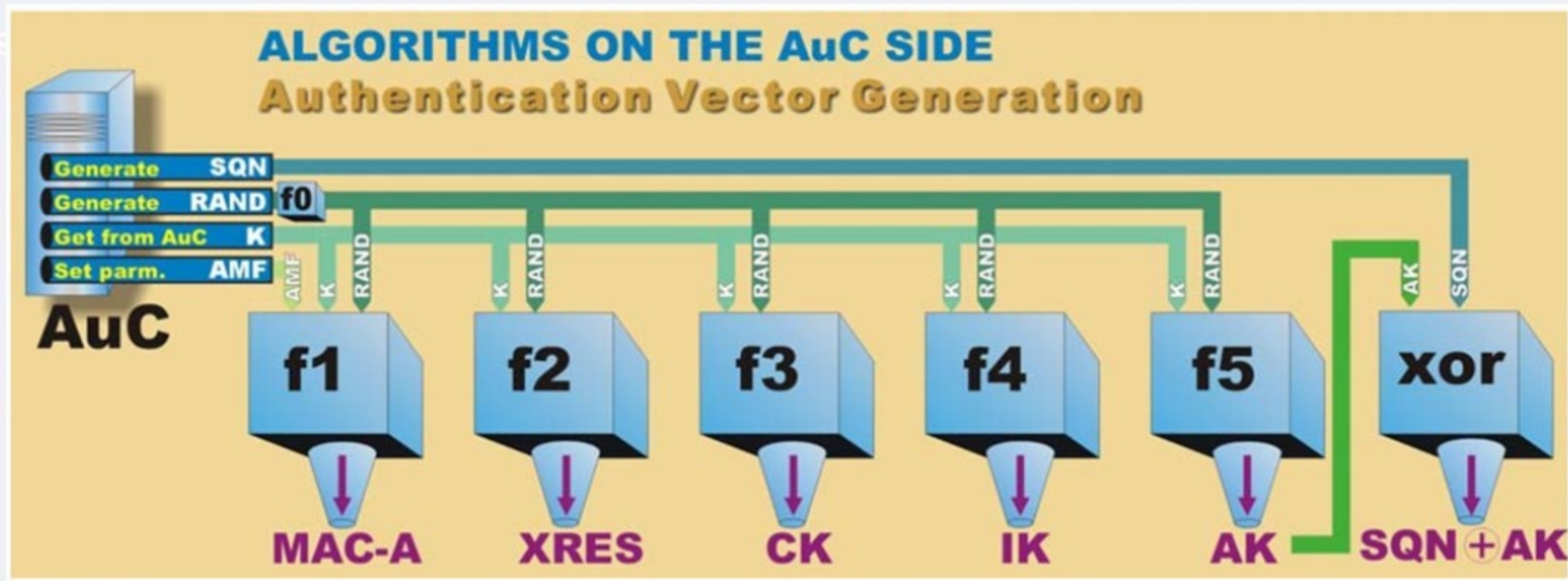
3G a LTE

Funkcia	Popis	Výstup	Lokácia	Status	Bit
f0	Náhodné čísla	RAN	AuC	Op. špec.	128
f1	Sieťová autentifikácia	(X)MAC-A	USIM, AuC	Op. Špec., (M)	64
f1*	Sieťová autentifikácia resynch.	(X)MAC-S	USIM, AuC	Op. Špec., (M)	64
f2	Užívateľská autentifikácia	RES/XRES	USIM, AuC	Op. Špec., (M)	32-128
f3	Derivácia kľúča pre šifru	CK	USIM, AuC	Op. Špec., (M)	128
f4	Derivácia kľúča pre integritu	IK	USIM, AuC	Op. Špec., (M)	128
f5	Derivácia kľúča pre anonymitu	AK	USIM, AuC	Op. Špec., (M)	48
f5*	Derivácia kľúča pre anonymitu resynch.	AK	USIM, AuC	Op. Špec., (M)	48
f8	Šifrovacia funkcia	...	MS, RNC	PŠ(K,S,AES)	
f9	Generovanie pečiatky integrity	MAC-I/XMAC-I	MS, RNC	PŠ(K,S,AES)	32
K	Kľúč na USIM – zdieľaný s AuC	Žiadny	USIM, AuC		128

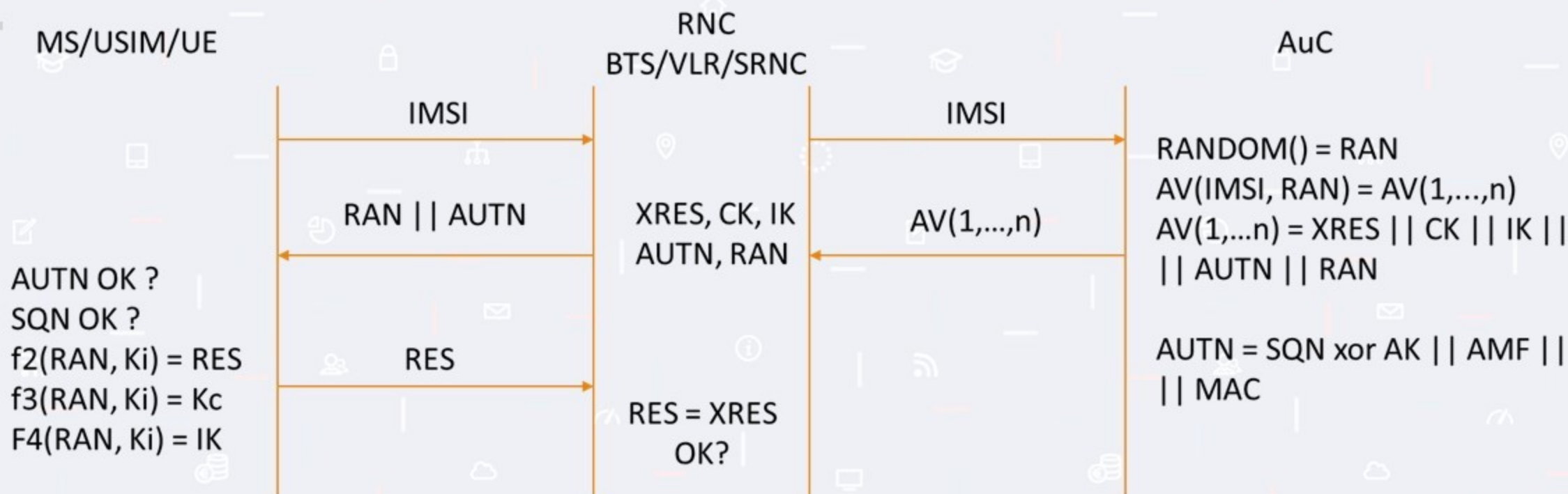
Algoritmy

- GSM:
 - ENC: A5/1 & A5/2
 - COMP128: A3 – 32 bit, A8 – 64 bit
 - Utajované
- 3G:
 - ENC: KASUMI (GEA0, GEA1) -> RNC CHOOSE ENC. -> MS
 - f9: Milenage
- 4G:
 - ENC: Snow 3G || AES 128b.

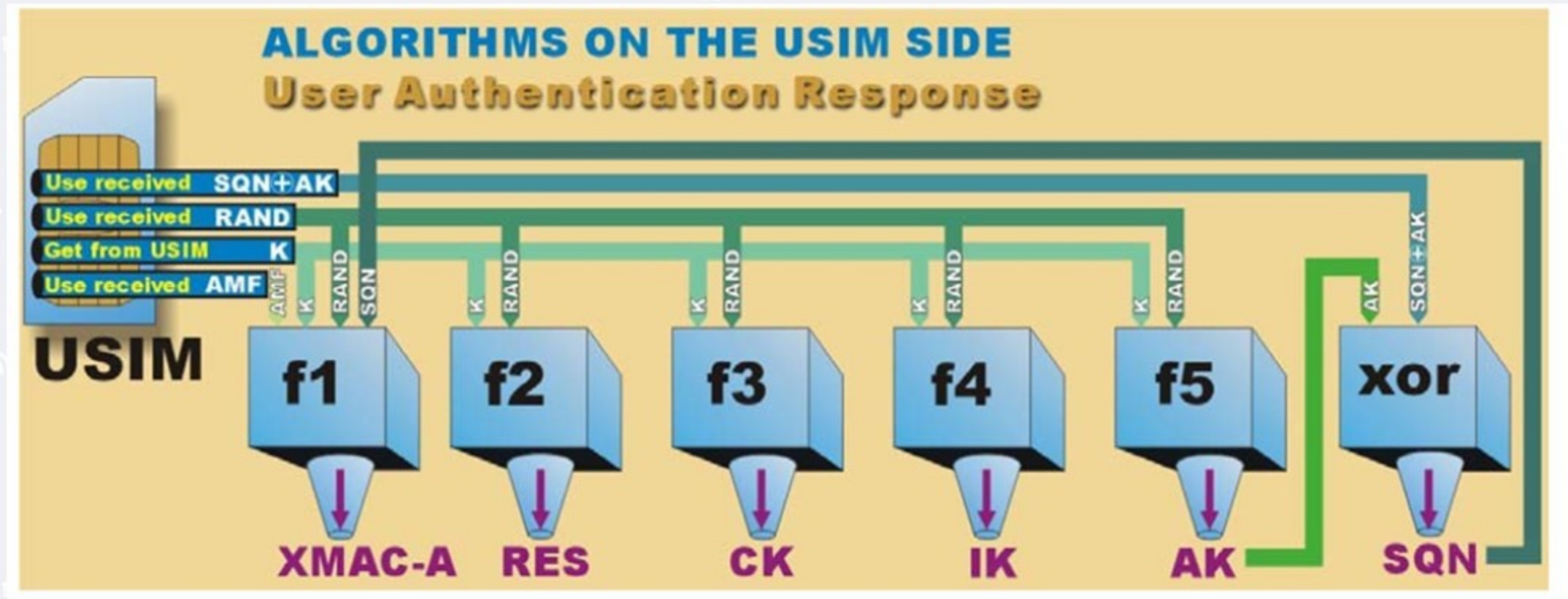
3G a LTE



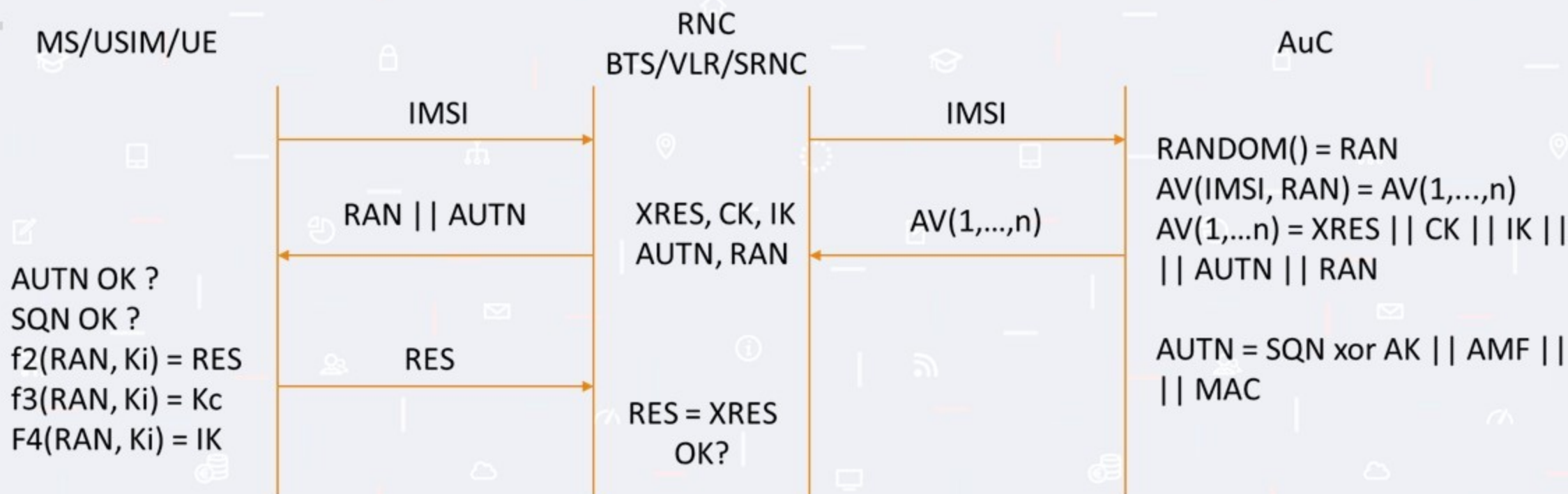
3G a LTE



3G a LTE

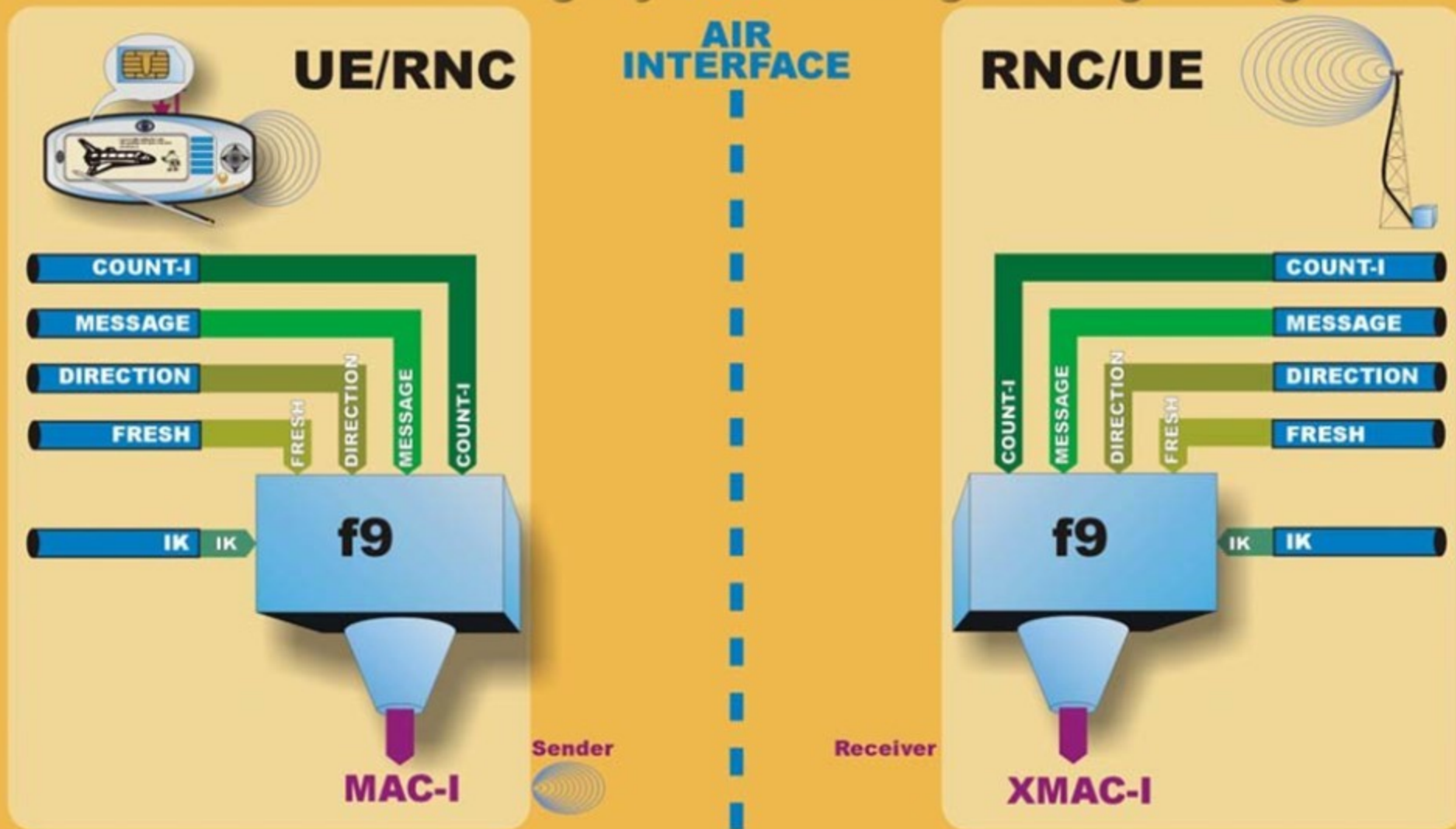


3G a LTE



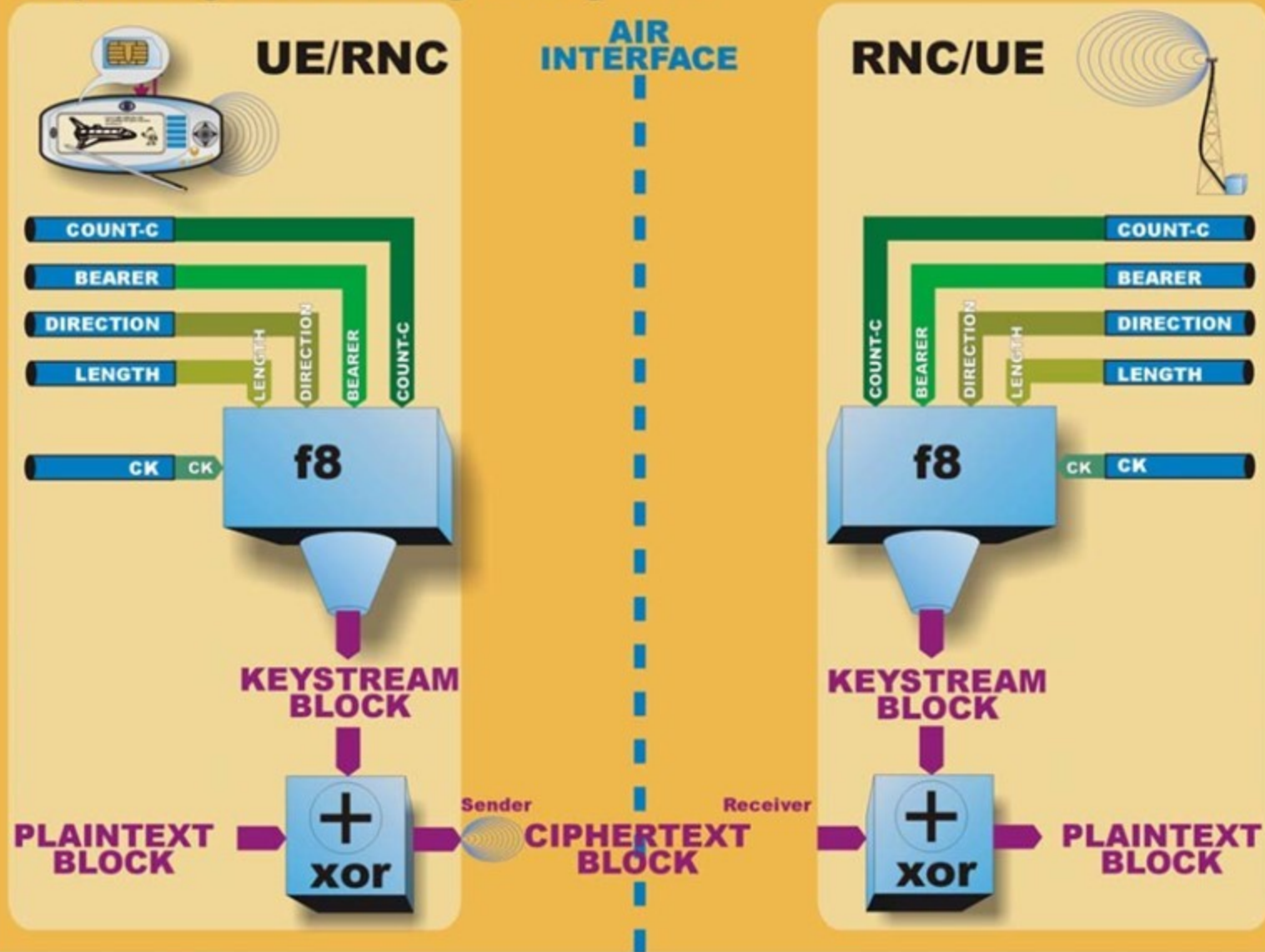
ALGORITHMS USED OVER THE RADIO ACCESS LINK

Authenticate data integrity and data origin of signalling data



ALGORITHMS USED OVER THE RADIO ACCESS LINK

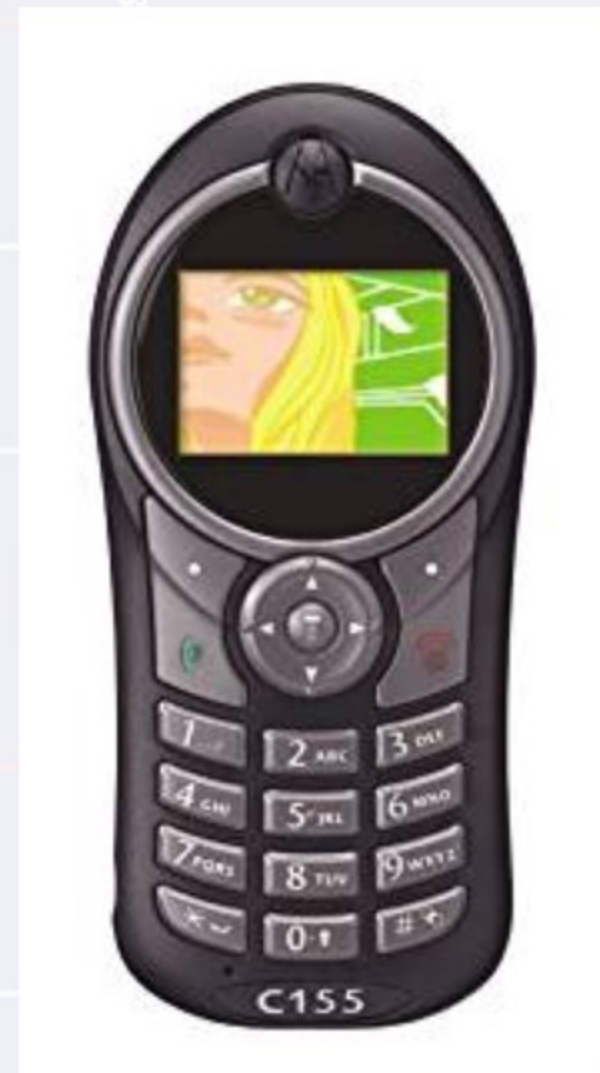
Ciphering user and signalling data



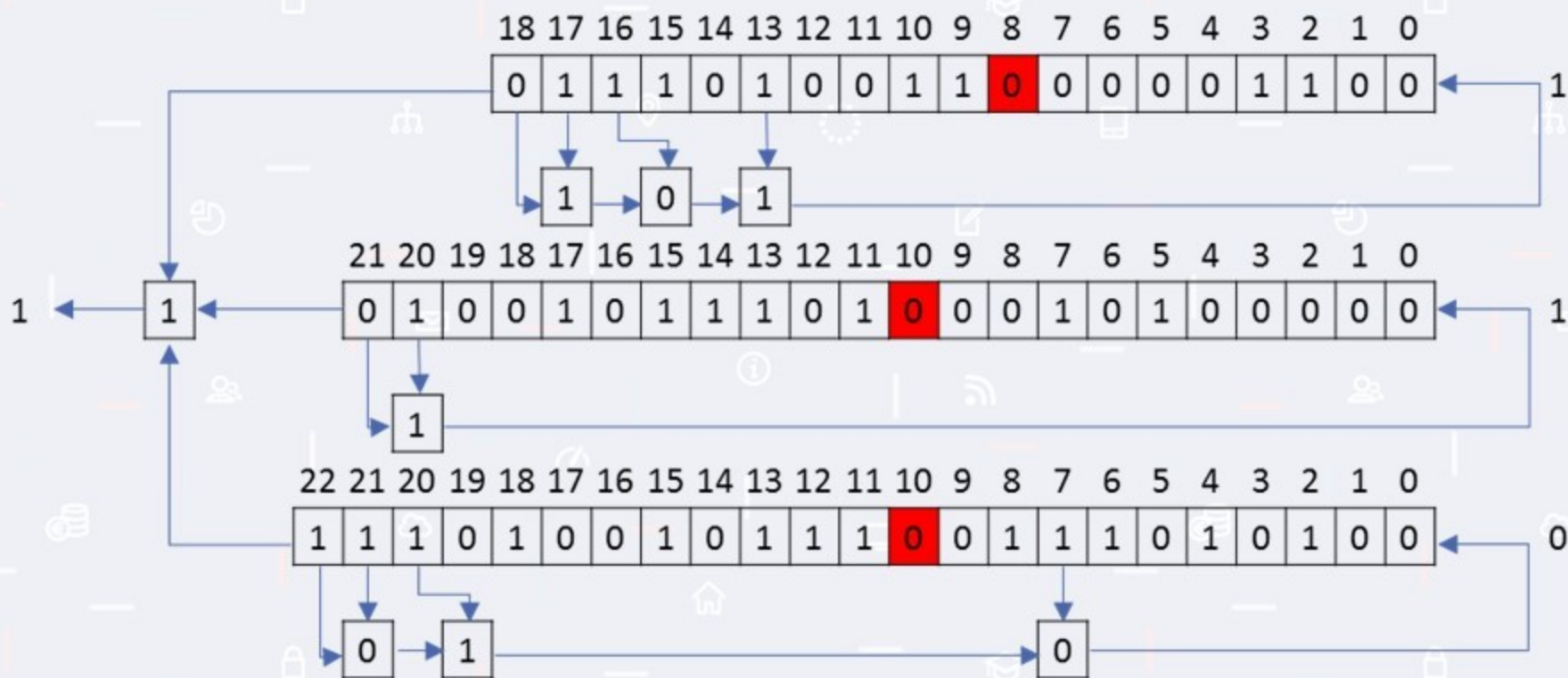
Lamanie A5/1
Rainbow tables
Time memory data tradeoff

A5/1

- Prúdové šifry
- Kryptoanalýza v reálnom čase
- BTS simulácia
 - Náročná implementácia
 - bb.osmocom.org
 - 5x Motorola C155 15\$ || bladeRF x40 420\$
- RTL-SDR
- Armáda (agáta)



A5/1



A5/1

- 2^{61} - počet možných stavov
- Chris Paget a Karsten Nohl
 - 2 TB predpočítaných dát
 - Zdieľané známou P2P sieťou
 - Pár sekúnd = prelomená A5/1
- Time-memory-data tradeoff
 - S určitou pravdepodobnosťou
 - Rainbow table
- NOP správy
- Detekovanie kľúča

A5/1 Time-Memory-data tradeoff

64b

000...1 → Koncový bod

000...2 → Koncový bod

000...3 → Koncový bod

.

.

.

fff...f → Koncový bod

A5/1 Time-Memory-data tradeoff

2^{64}

64b
000...1 → Koncový bod
000...2 → Koncový bod
000...3 → Koncový bod
.
.
.
fff...f → Koncový bod



A5/1 Time-Memory-data tradeoff

64b

000...1 → A5/1 → A5/1 ... → A5/1 → Koncový bod

000...2 → A5/1 → A5/1 ... → A5/1 → Koncový bod

000...3 → A5/1 → A5/1 ... → A5/1 → Koncový bod

.

.

fff...f → A5/1 → A5/1 ... → A5/1 → Koncový bod



A5/1 Time-Memory-data tradeoff

64b

000...1 → A5/1 → A5/1 ... → A5/1 → ...0000

000...2 → A5/1 → A5/1 ... → A5/1 → ...0000

000...3 → A5/1 → A5/1 ... → A5/1 → ...0000

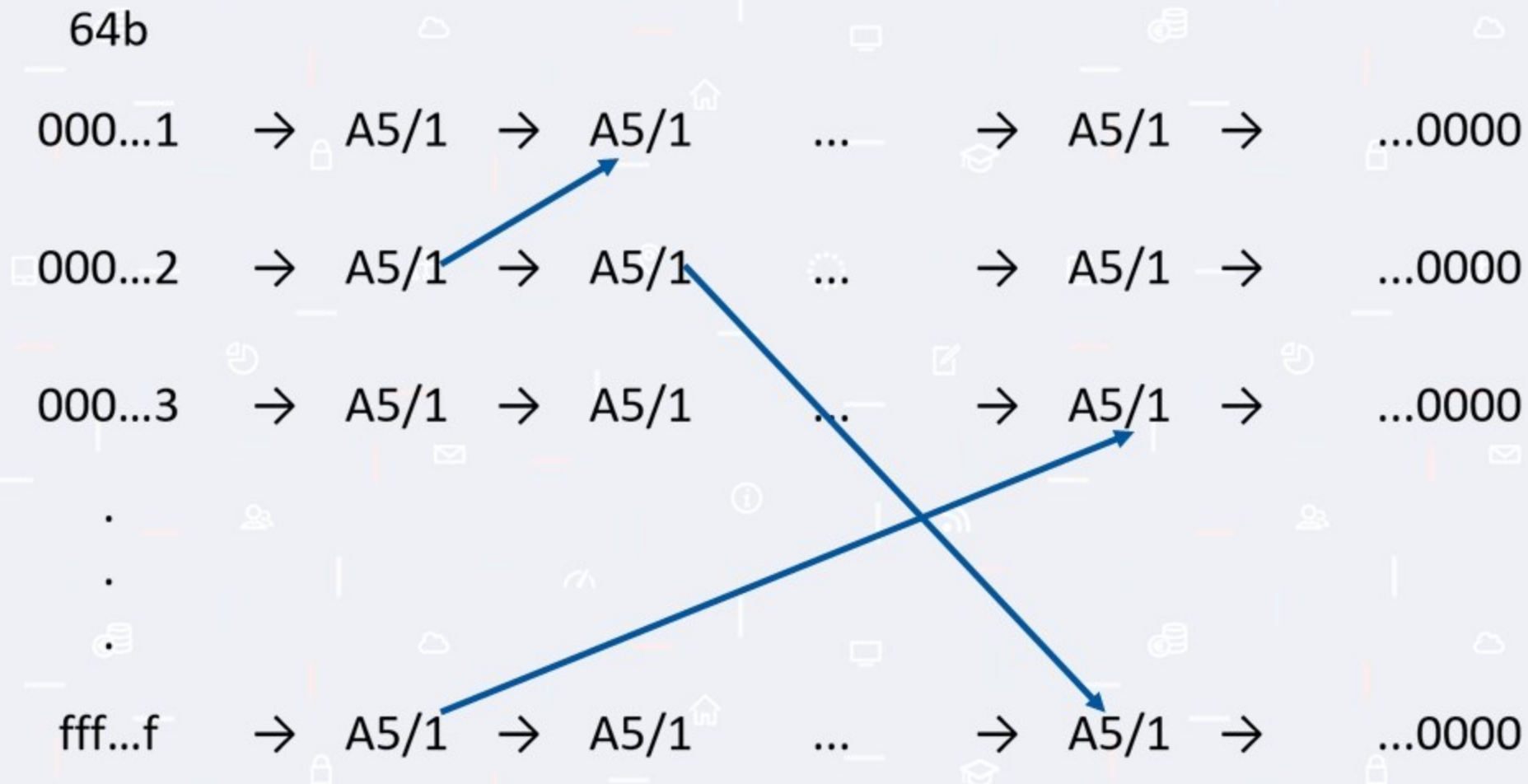
.

.

fff...f → A5/1 → A5/1 ... → A5/1 → ...0000



A5/1 Time-Memory-data tradeoff



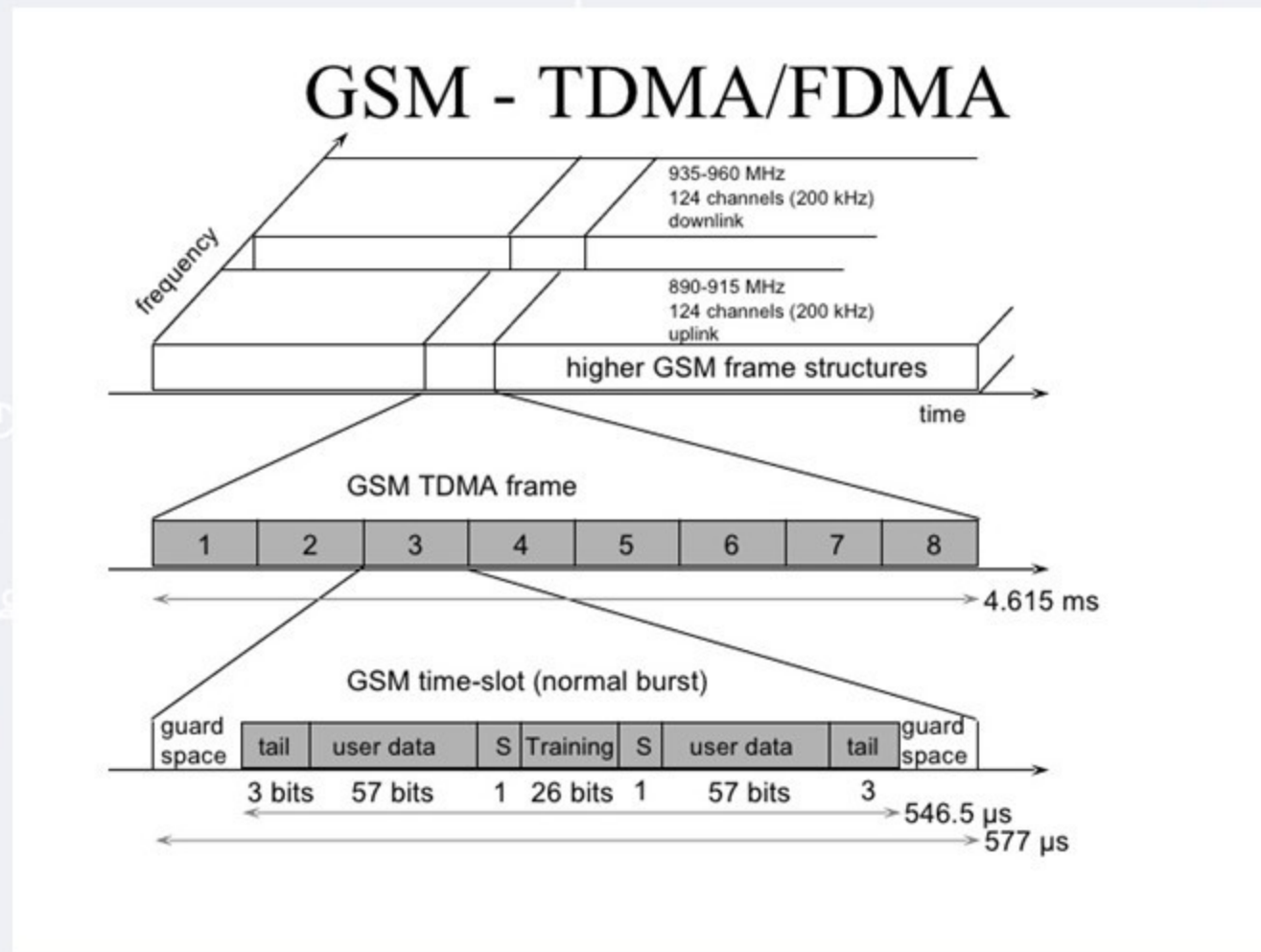
A5/1 Time-Memory-data tradeoff



A5/1

- 2^{61} - počet možných stavov
- Naivná tabuľka: 296 EB (exabajt)
- Zredukovanie vnútorných stavov o 3 bity (efektívny počet bitov): 37 EB
- GSM Frame 4x po 114 bitov – potrebujeme len 64 => 204 rôznych posunov
37/204
- Zavedenie 4096 blokov -> $37/204/4096 = 44$ TB
- Zavedenie 8 farieb = 5,5 TB
- Zredukovanie výšky tabuľky na 2^{34} a použijeme hash
- Zakódovanie endpointu = 1.8T

Frame, burst



Správy nop

- Fixný text
- Nemám ti čo povedať, ale niečo hovorím 😊

NOP

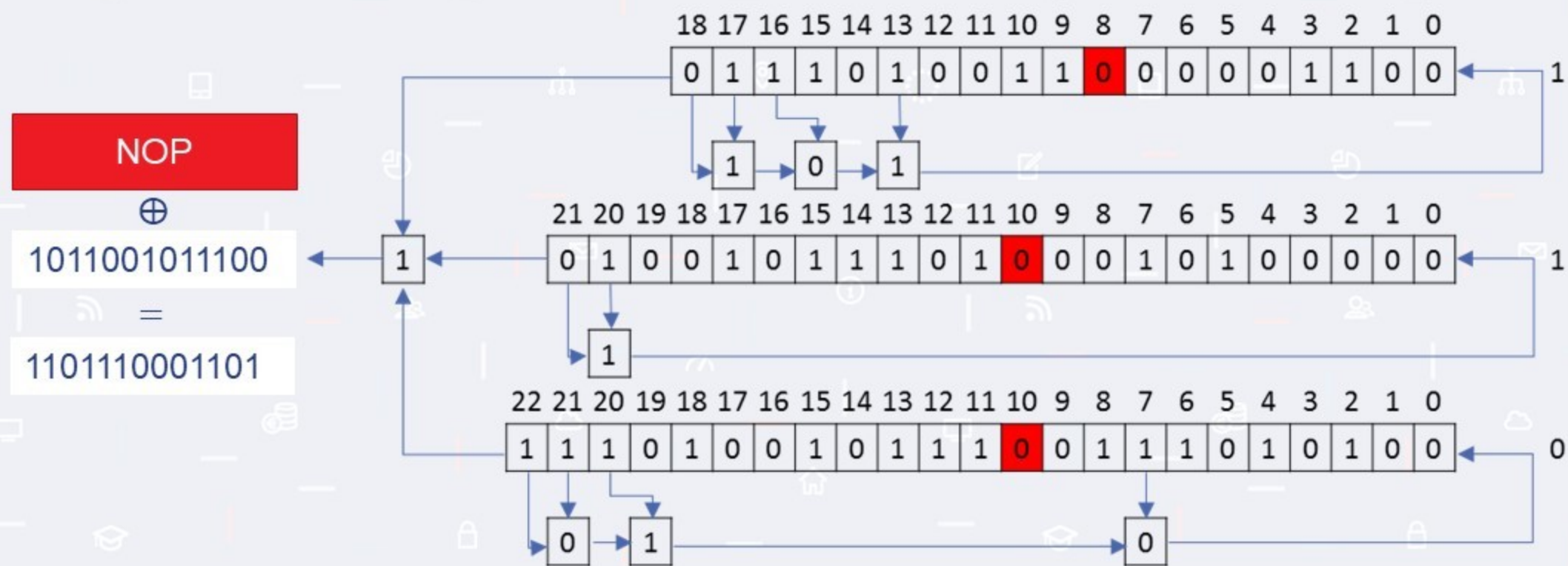


Keystream 1

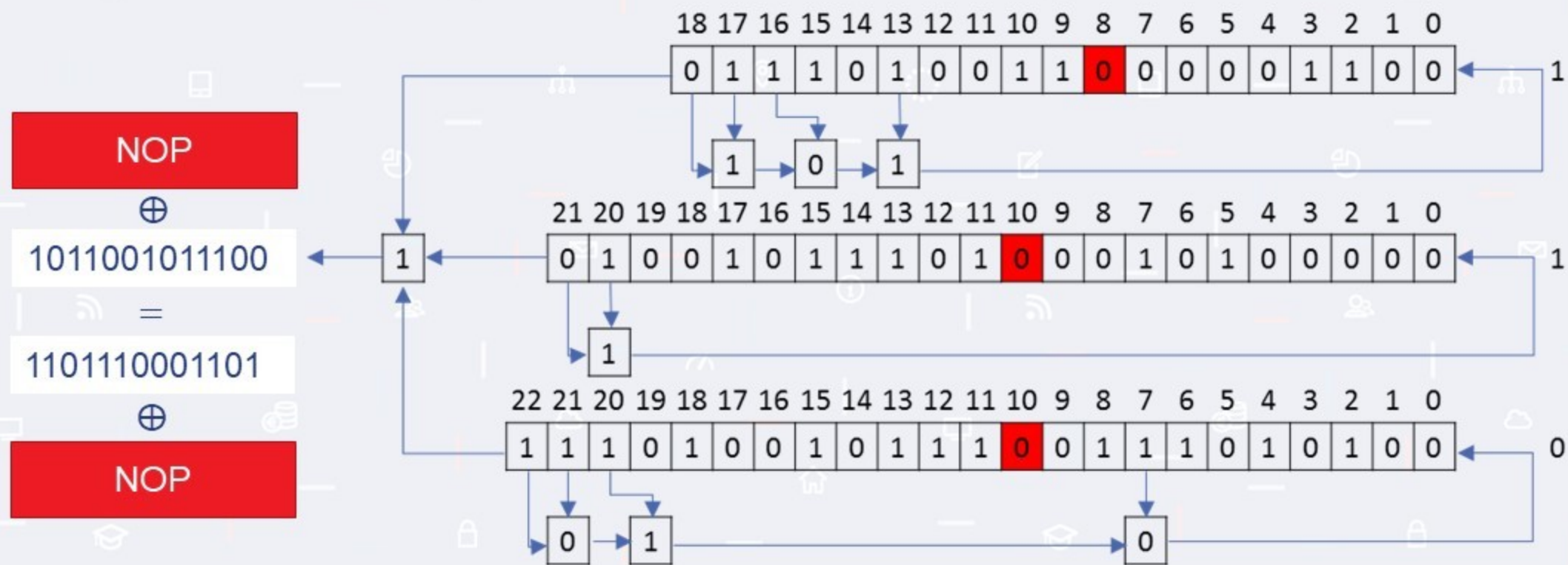
= BURST (114bitov)



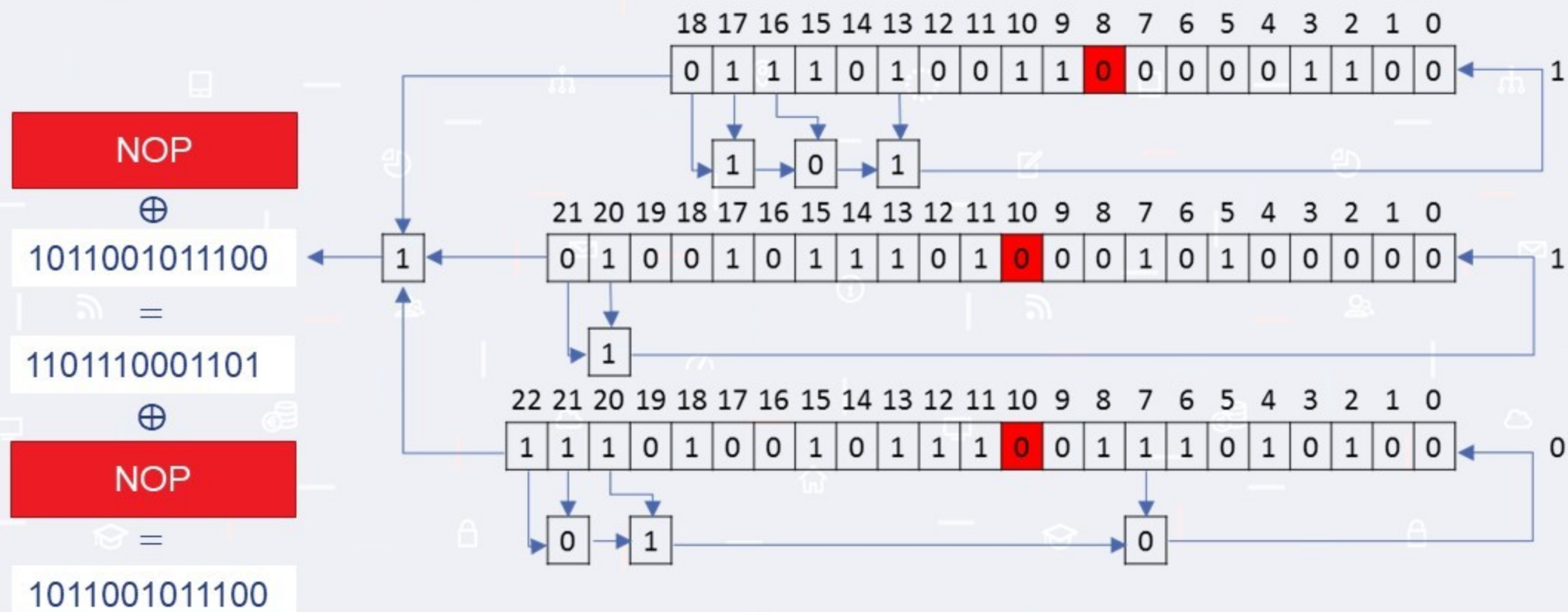
A5/1



A5/1



A5/1



XOR operácie

1	$\oplus$	1	0
1	$\oplus$	0	1
0	$\oplus$	1	1
0	$\oplus$	0	0

NOP

$\oplus$

1011001011100

=

1101110001101

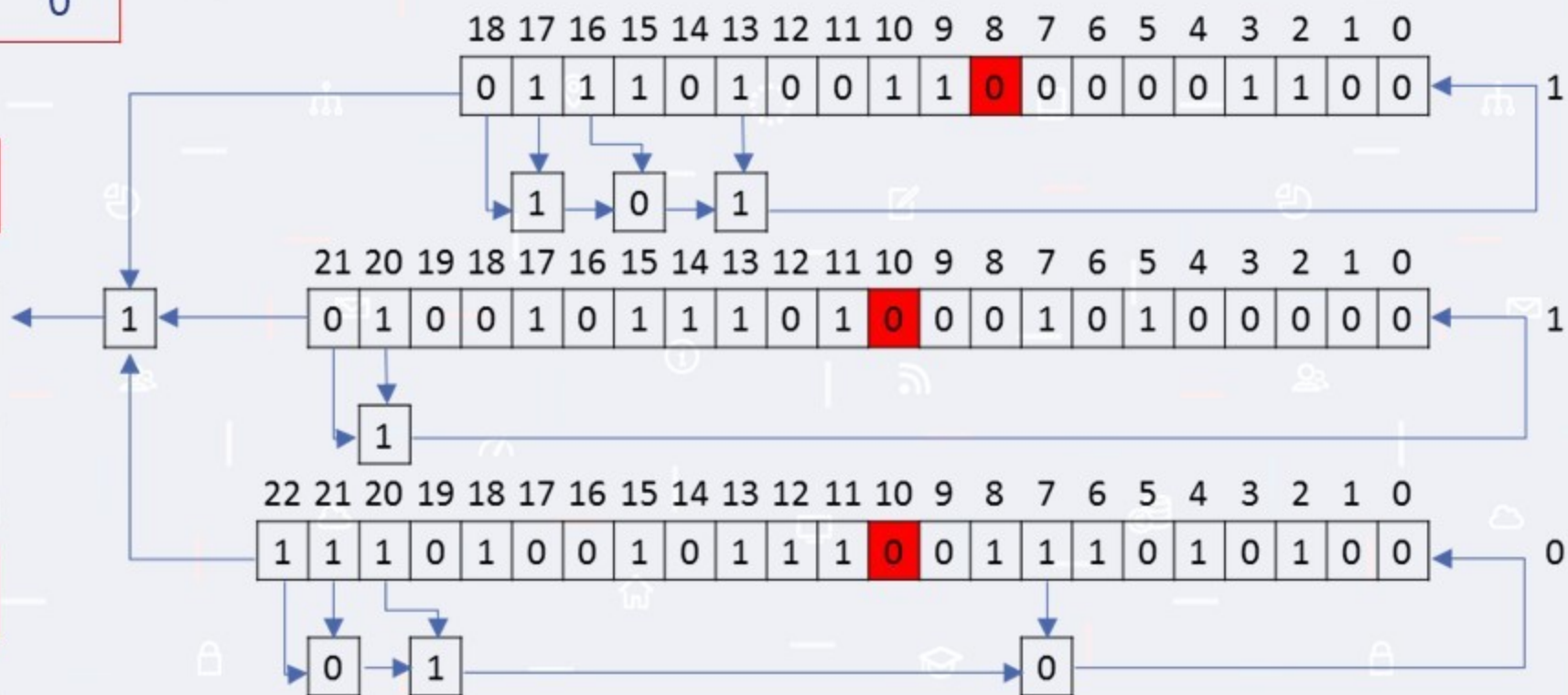
$\oplus$

NOP

=

1011001011100

A5/1



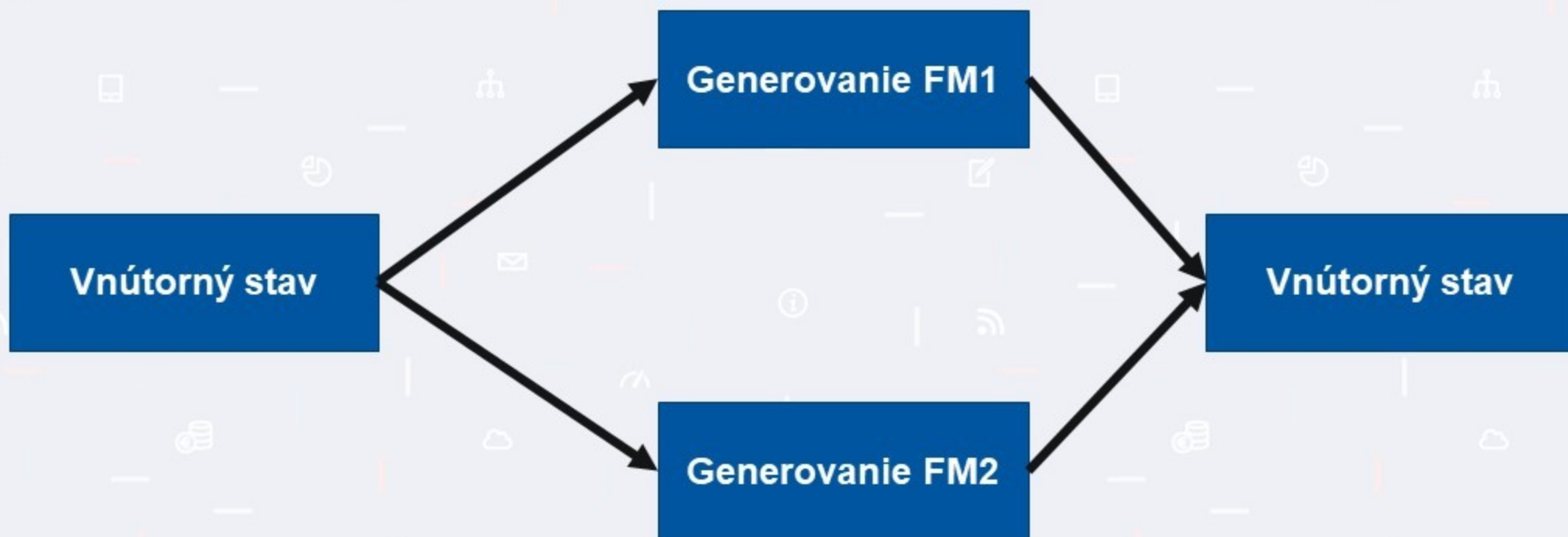
Frame

- Každý frame má svoje číslo
- Číslo je verejné známe
- Každý frame ma niekoľko burstvo
- Každý burst je šifrovaný individuálne

Frame update

- Každý frame má svoje číslo
- Číslo je verejné známe
- Každý frame ma niekoľko burstvo
- Každý burst je šifrovaný individuálne
- NOP ma nahodný padding
 - rainbow tabuľky na základe frame number

Dešifrovanie na základe Frame number



Ďalšie možnosti

- Snoopsnitch
- SS7 protokol
- IMSI catcher
- Falošná BTS
- Falošný operátor
- ...

Zdroje

- https://brage.bibsys.no/xmlui/bitstream/handle/11250/137418/master_ikt_2001_dohmen.pdf?sequence=1
- http://www.netlab.tkk.fi/opetus/s38153/k2003/Lectures/g42UMTS_security.pdf

Pre 4G (LTE):

- <http://www.ijritcc.org/download/1430372773.pdf>

Klonovanie (U)SIM kariet:

- <https://www.blackhat.com/docs/us-15/materials/us-15-Yu-Cloning-3G-4G-SIM-Cards-With-A-PC-And-An-Oscilloscope-Lessons-Learned-In-Physical-Security.pdf>

**Ďakujem
za pozornosť**

