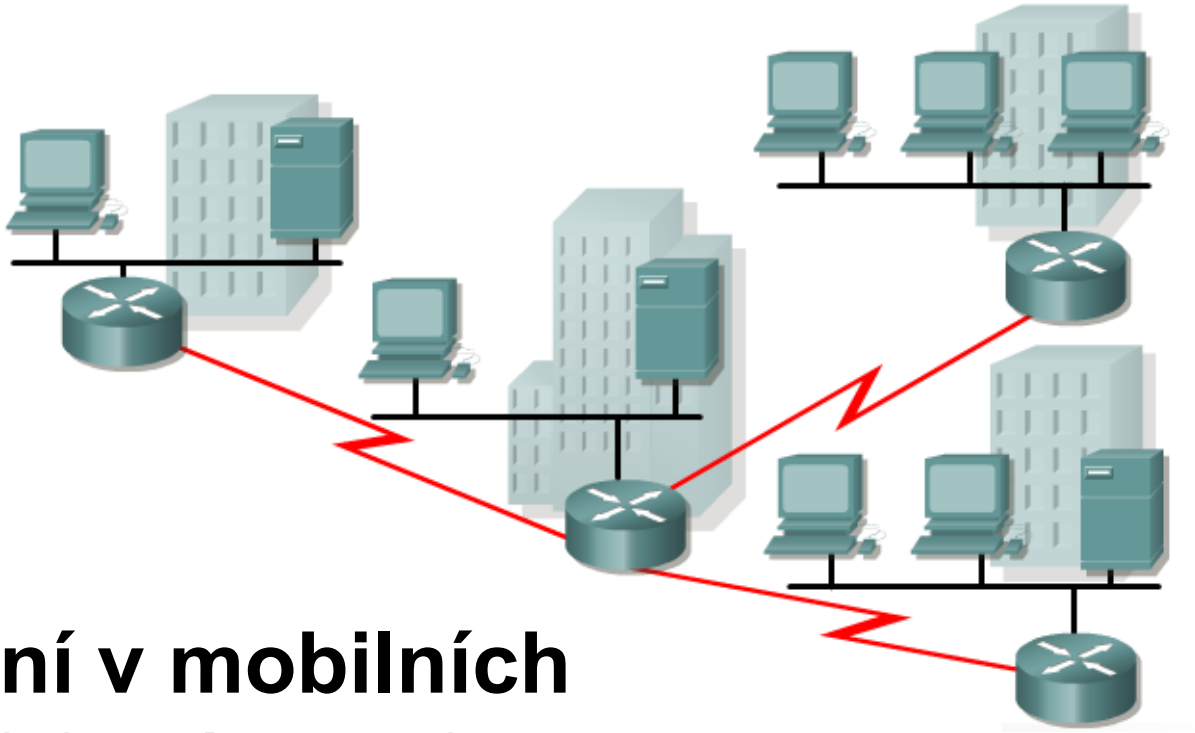


# Zabezpečení v mobilních sítích GSM / UMTS

Ing. Tomáš Vaněk, Ph.D.
tomas.vanek@fel.cvut.cz

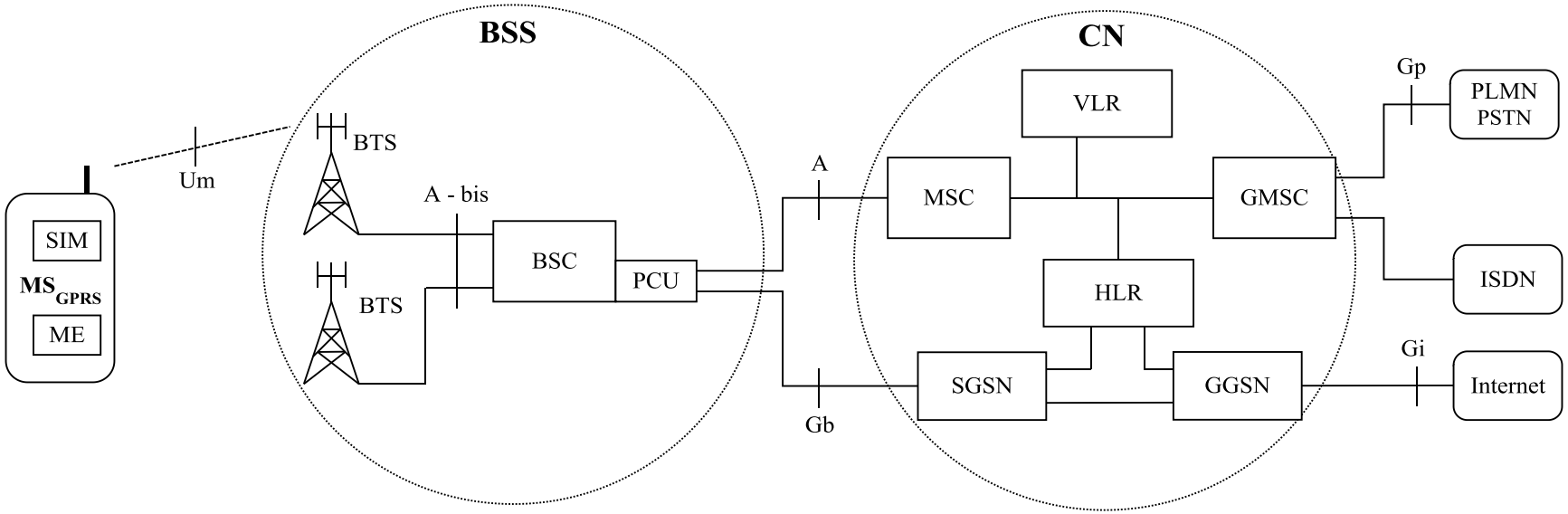
# GSM

- Anonymita
- Autentizace
- Šifrování
- Integrita

# Specifikace GSM byly vyvíjeny neveřejně

- Žádné veřejné hodnocení a diskuze
- Porušení Kerckhoffova principu: Bezpečnost algoritmu by měla záviset výhradně na utajení klíče a nikoliv na utajení samotného algoritmu
- Specifikace GSM i šifrovacích algoritmů nakonec stejně unikly a byly v nich objeveny bezpečnostní díry

# Struktura GSM sítě




BSS - Base Station Subsystem

CN – Core Network

MS – Mobile Station

BSC – Base Station Controller

BTS – Base Transiever Station

MSC – Mobile Switching Center

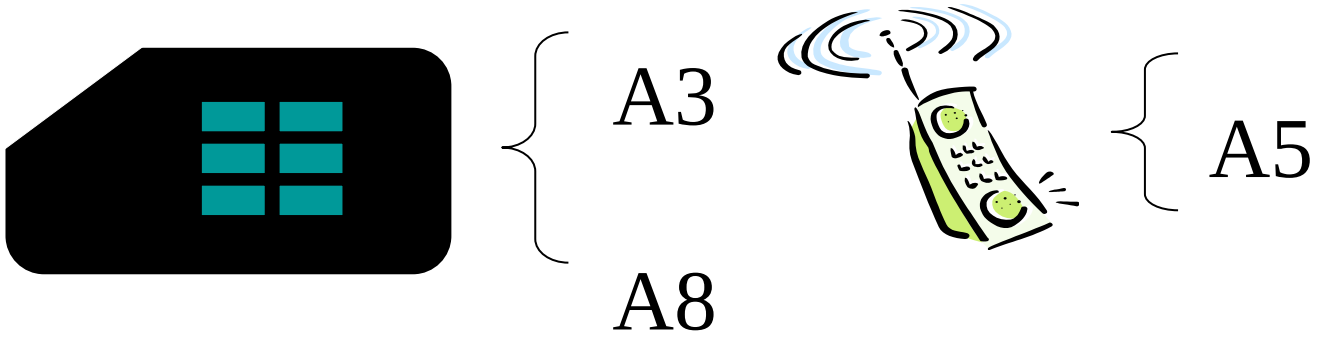
HLR – Home Location Register

VLR – Visitors  Location Register

SGSN – Switching GPRS Servis Node

GMSC/GGSN – Gateway pro MSC , SGSN

# Šifrovací algoritmy v GSM karta SIM




Algoritmy, které jsou používány pro šifrování v mobilní síti GSM:

- A3 - autentizační algoritmus
- A5 - šifrovací algoritmus
- A8 - generátor klíče pro hlasovou komunikaci

Karta SIM obsahuje ještě tajný klíč $K_i$, který je uložen i v AuC.

# Bezpečnostní model GSM sítě

## IMSI – International Mobile Subscriber Identity

- identifikace účastníka
- uloženo na SIM kartě
- skládá se ze 3 částí:
  1. Mobile Country Code (MCC) - 230
  2. Mobile Network Code (MNC)

| | | |
|---|---|---|
| T-mobile | 01 | |
| O2 CZ | 02 | |
| Vodafone | 03 | |
| U:fon | 04 | |
| SDŽC | 98 | (Správa železniční dopravní cesty) |
| Vodafone | 99 | |

  3. MSIN - Mobile Subscriber Identity Number („telefonní číslo)

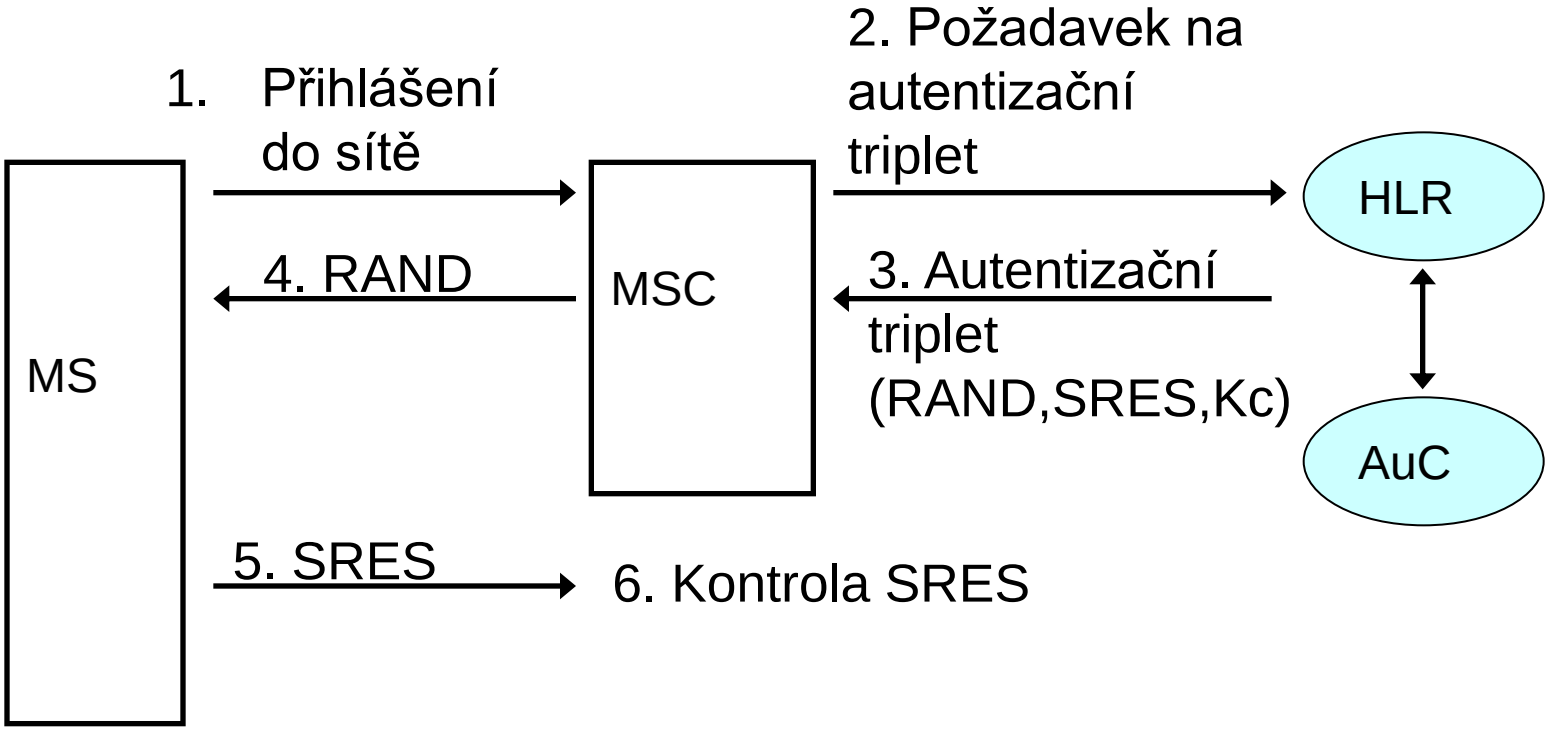
# Bezpečnostní model GSM sítě

- IMSI je globálně jednoznačný
- Při komunikaci MS-síť se nepoužívá IMSI
  - bylo by možné sledovat, kde se nachází konkrétní uživatel
- používá se TMSI (Temporary IMSI) / P-TMSI
  - Má pouze lokální platnost (pouze v rámci LA (RA), kde je účastník zaregistrován)
  - Vazba IMSI-TMSI/P-TMSI udržována ve VLR/SGSN
  - *TMSI* je používána při požadavcích na:
    - paging
    - aktualizaci lokační oblasti
    - Spojení
    - opětovné navázaní spojení
    - ukončení spojení…
  - Snižuje možnost monitorování a sledování účastníků

# Autentizace v GSM

- Kdo: SIM karta
  AuC (Authentication Center ) – v domácí síti
- Jednosměrná autentizace MS->síť
- Založeno na tajném klíči Ki - 128 bitů
- Ki uložen pouze na SIM a v AuC
- Autentizace se odehrává vždy v domácí síti !!
  - Autentizační algoritmus je nezávislý na samotné mobilní síti, ve které probíhá.
  - Proto autentizace funguje i v cizích sítích.
- Autentizace typu „challenge-response“.
- Používá algoritmus A3.

# Autentizace v GSM síti




SRES = A3(RAND,Ki)

Kc = šifrovací klíč pro komunikaci MS<->BTS

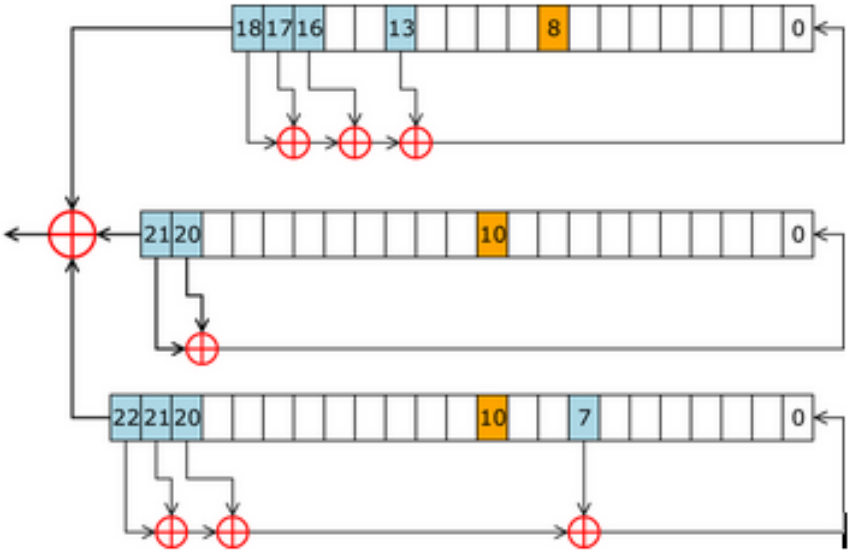
# Šifrování v GSM

Kde: Šifrování na rádiovém rozhraní sítě mezi MS a BTS

- šifrovací algoritmus A5 je uložen v MS
- je stejný pro všechny operátory (proč ?)
- klíč je generován algoritmem A8 uloženým na SIM -> algoritmus A8 si může operátor zvolit
- vstup do A5:
  - relační klíč $K_c$ = A8(RAND, $K_i$) délky 64 bitů
  - číslo TDMA rámce (22 bitů)
- výstup: 114 bitů
- A5 – proudová šifra, resynchronizovaná každý rámec
- $K_c$ - nemění se často (pouze při autentizaci)
- jediné šifrované rozhraní v celé GSM síti

# A5/1

- A5/1 obsahuje of 3 *posuvné registry*
  - X: 19 bitů ($x_{18},x_{17},x_{16}, \ldots,x_0$)
  - Y: 22 bitů ($y_{21},y_{20},y_{19}, \ldots,y_0$)
  - Z: 23 bitů ($z_{22},z_{21},z_{20}, \ldots,z_0$)




- klíčem je počáteční hodnota registrů
- každá buňka obsahuje 1 bit
- v každém kroku se registr posune nebo zůstane stát
- proud klíče vzniká XORem výstupu tří registrů

# A5

Proudový algoritmus  A5/1 používá tři LFSR. Registr se posune pokud hodnota jeho „hodinového bit“ (oranžový) souhlasí s většinovou hodnotou všech „hodinových bitů“.

Algoritmus A5/1 je založen na kombinaci tří lineárních registrů se zpětnou vazbou  (LFSR) a nepravidelného časování.

# A5

Na počátku jsou registry vynulovány. Poté je v 64 krocích namixován 64 bitový tajný klíč Ki podle následujícího principu:
Pro 0<i<64, je *í-tý* bit klíče přidán do každého registru pomocí operace XOR : R[i]=R[i] XOR K[i]

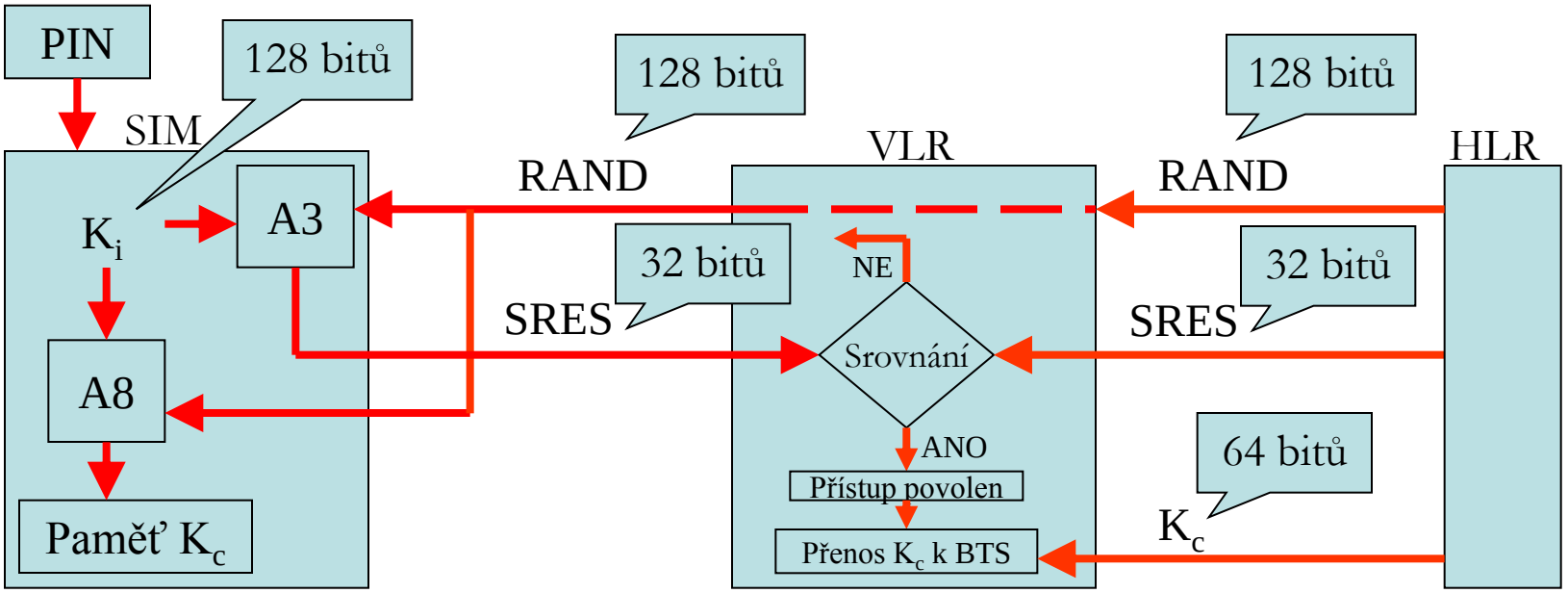
Poté je každý registr posunut. Po načtení klíče se do systému přičte 22 bitů čísla rámce a poté je systém provozován 100 hodinovým taktů s odpojeným výstupem. Poté je systém připraven vyprodukovat 228 bitů výstupního proudu klíče.

# Varianty A5

Existuje několik verzí algoritmu A5, které poskytují různou úroveň zabezpečení:

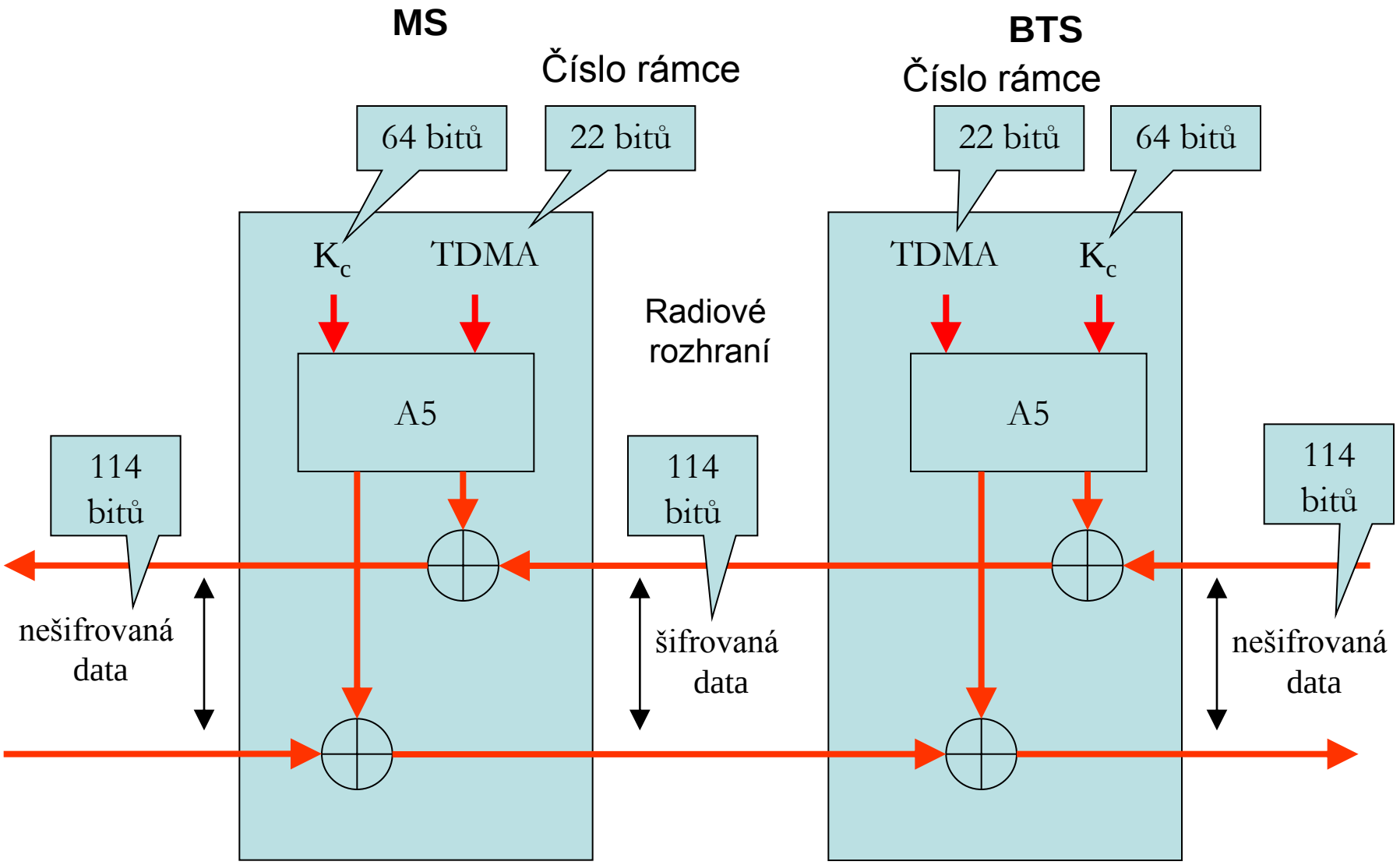
- A5/0 – neposkytuje žádné zabezpečení
- A5/1 – původní algoritmus A5 používaný v Evropě
  - prvních deset bitů klíče je nulových
  - efektivní délka klíče – 54 bitů
- A5/2 – kryptograficky oslabená varianta algoritmu vytvořená pro export a používaná v USA
- A5/3 (Kasumi) – silný šifrovací algoritmus vytvořený jako součást 3rd Generation Partnership Project (3GPP)

# Šifrovací algoritmy v GSM
# A3 a A8




A3/8, A38, COMP128 – různé názvy pro jeden algoritmus
ani A3, ani A8 nejsou specifikovány v doporučeních ETSI

# Šifrovací algoritmy v GSM
## A5



# Útoky na GSM

- 2003 – Barkan a kol. několik útoků na šifrování v GSM
  - aktivní útok – přesvědčit telefon aby změnil šifrování na A5/2
  - ciphertext-only TMTO – velký objem předpočítaných dat / chybí detailní popis útoku http://cryptome.org/gsm-crack-bbk.pdf
- 2006 - Barkan, Biham a Keller publikovali plnou verzi článku z roku 2003 o útocích na A5

  http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf
- 2007 - University v Bochuma v Kiely spustili projekt COPACOBANA – zařízení s mnoha FPGA

  http://www.copacobana.org/
- První komerčně dostupné zařízení ~ 10.000€ schopné zrealizovat výrazné urychlení TMTO pro útok na A5/1 A5/2 nebo DES (DES prolomí dnes za cca 7 dní)

# Útoky na A5

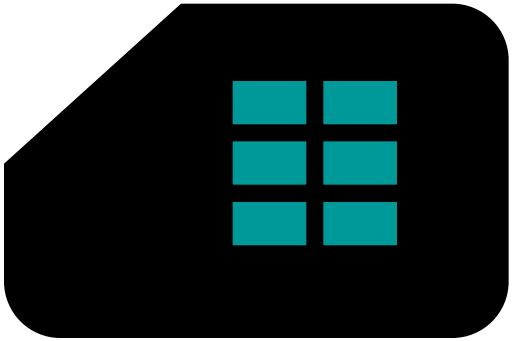
Projekt „A5/1 Rainbow table“

- http://reflextor.com/trac/a51/wiki
- cíl – vytvořit tabulky pro TMTO útok na GSM
- spuštěno v září 2009
- pomocí Nvidia GPU (12x GeForce GTX260)
- má být hotovo za cca 650 dní
- 25.10.2009 objevena chyba v interní implementaci A5 -> znovu a lépe

# GSM

- Anonymita – dobrá
- Autentizace – špatná
  - pouze jednosměrná
  - neexistuje schéma pro výměnu klíčů
  - předsdílené klíče
- Šifrování – špatné
  - krátký klíč
  - slabý algoritmus – lze prolomit (rainbow tables)
- Integrita - žádná

# Šifrovací algoritmy v UMTS
# karta USIM



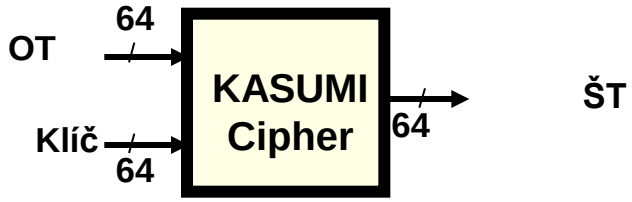
f1
f2
f3
f4
f5

f8
f9

Karta USIM obsahuje ještě tajný klíč K, který je uložen i v AuC.

# KASUMI

- bloková šifra pro f8,f9
- délka bloku 64 bitů
- délka klíče 128 bitů

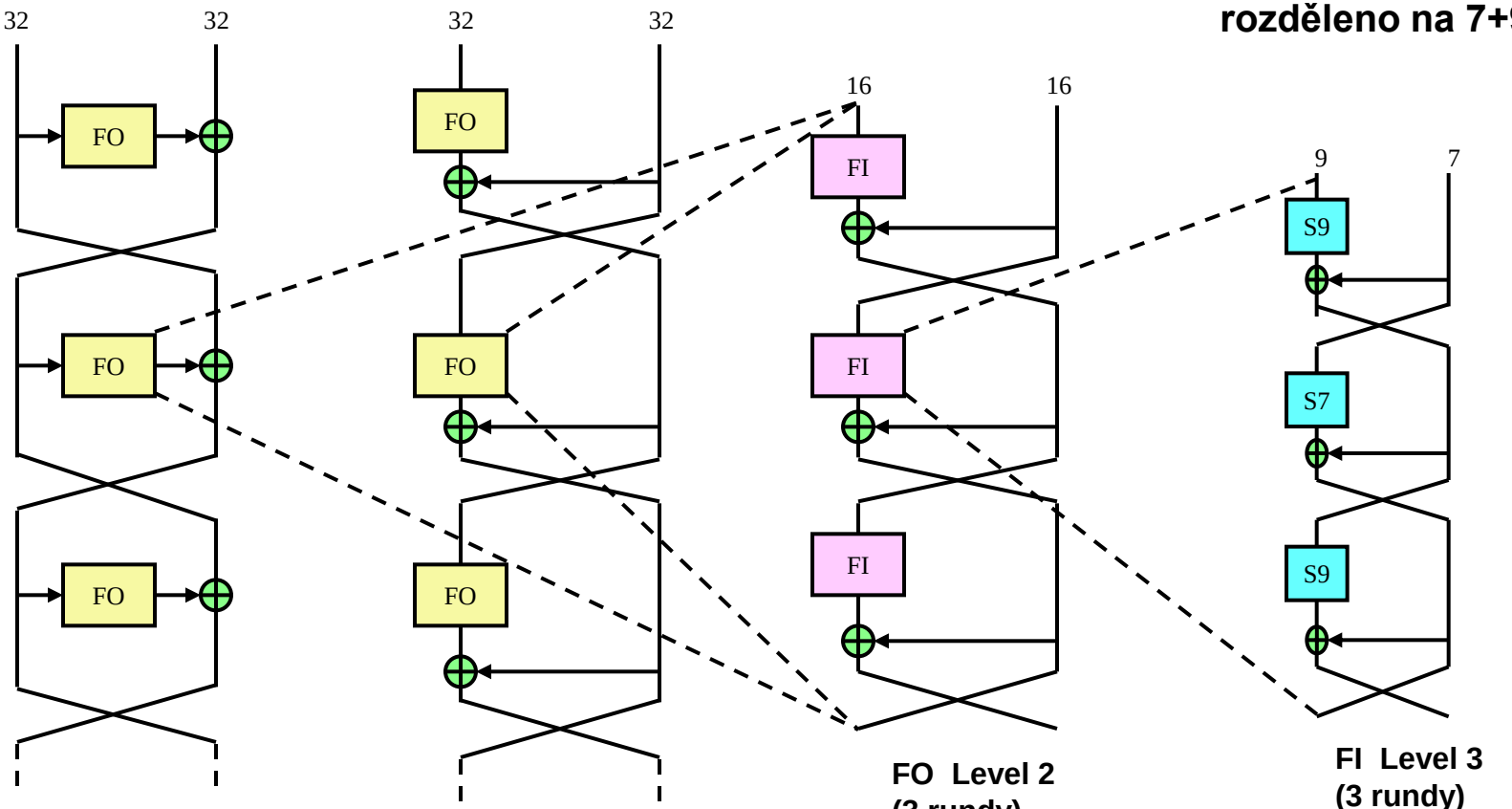



- různý počet rund (doporučeno 8)
- publikoval M.Matsui (Mitsubishi) v roce 1996
- březen 2000 – KASUMI byl zvolen jako povinný algoritmus pro utajování a zajištění integrity dat pro W-CDMA sítě sdružením 3GPP
- **KASUMI** variantou šifry **MISTY1 uzpůsobenou pro W-CDMA sítě**
- “KASUMI (japonsky)”=“MIST (mlha)”

- Vysoká bezpečnost – prokazatelně odolná vůči lineární a diferenciální kryptoanalýza
- Multi platformní – rychlé SW i HW implementace
- Kompaktní – malý rozměr čipu a nízká spotřeba (při HW realizaci)
- Použití:
  - ISO9979 No.13
  - možný algoritmus v TLS
  - rozšířené S/MIMEv2
  - šifrovací schéma pro PKCS#5 (Password-based Encryption)
  - šifrovací algoritmus v PKCS#7 (Cryptographic Message Syntax Standard)

# Rekurzivní struktura MISTY

**16 vstupních bitů je rozděleno na 7+9**




**MISTY1 Level 1**
**(n rund)**

**MISTY2 Level 1**
**(n rund)**

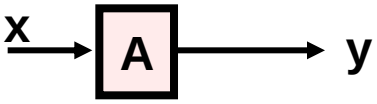
**FO Level 2**
**(3 rundy)**

**FI Level 3**
**(3 rundy)**

# 16 vstupních bitů je rozděleno na ( 7 + 9 ) bitů které se mapují na tabulky S7 a S9

## Tabulka S7 nad $F_2^9$

27, 50, 51, 90, 59, 16, 23, 84, 91, 26,114,115,107, 44,102, 73,
31, 36, 19,108, 55, 46, 63, 74, 93, 15, 64, 86, 37, 81, 28, 4,
11, 70, 32, 13,123, 53, 68, 66, 43, 30, 65, 20, 75,121, 21,111,
14, 85, 9, 54,116, 12,103, 83, 40, 10,126, 56, 2, 7, 96, 41,
25, 18,101, 47, 48, 57, 8,104, 95,120, 42, 76,100, 69,117, 61,
89, 72, 3, 87,124, 79, 98, 60, 29, 33, 94, 39,106,112, 77, 58,
1,109,110, 99, 24,119, 35, 5, 38,118, 0, 49, 45,122,127, 97,
80, 34, 17, 6, 71, 22, 82, 78,113, 62,105, 67, 52, 92, 88,125




**Mapy S7 a S9 jsou generovány pomocí vztahu :**

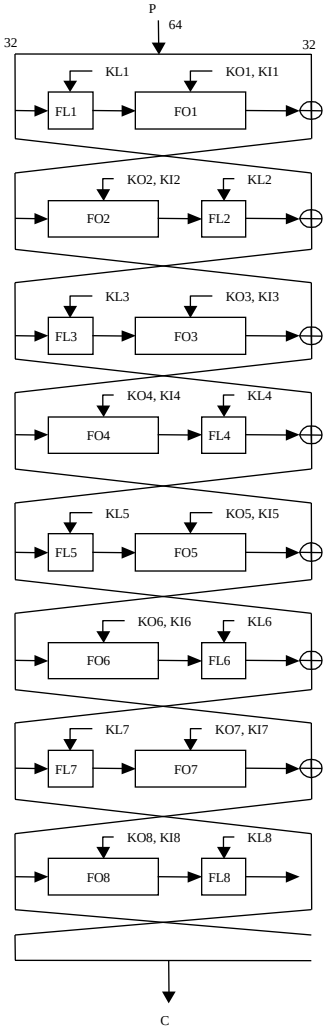
**$Y = A(x^i)$ v poli $F_2^7$ a $F_2^9$**

## Tabulka S9 nad $F_2^9$

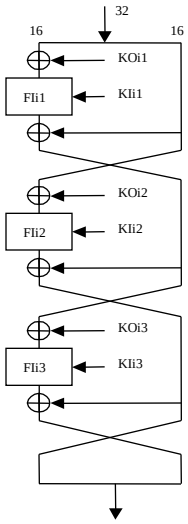
451,203,339,415,483,233,251, 53,385,185,279,491,307, 9, 45,211,
199,330, 55,126,235,356,403,472,163,286, 85, 44, 29,418,355,280,
331,338,466, 15, 43, 48,314,229,273,312,398, 99,227,200,500, 27,
1,157,248,416,365,499, 28,326,125,209,130,490,387,301,244,414,
467,221,482,296,480,236, 89,145, 17,303, 38,220,176,396,271,503,
231,364,182,249,216,337,257,332,259,184,340,299,430, 23,113, 12,
71, 88,127,420,308,297,132,349,413,434,419, 72,124, 81,458, 35,
317,423,357, 59, 66,218,402,206,193,107,159,497,300,388,250,406,
481,361,381, 49,384,266,148,474,390,318,284, 96,373,463,103,281,
101,104,153,336, 8, 7,380,183, 36, 25,222,295,219,228,425, 82,
265,144,412,449, 40,435,309,362,374,223,485,392,197,366,478,433,
195,479, 54,238,494,240,147, 73,154,438,105,129,293, 11, 94,180,
329,455,372, 62,315,439,142,454,174, 16,149,495, 78,242,509,133,
253,246,160,367,131,138,342,155,316,263,359,152,464,489, 3,510,
189,290,137,210,399, 18, 51,106,322,237,368,283,226,335,344,305,
327, 93,275,461,121,353,421,377,158,436,204, 34,306, 26,232, 4,
391,493,407, 57,447,471, 39,395,198,156,208,334,108, 52,498,110,
202, 37,186,401,254, 19,262, 47,429,370,475,192,267,470,245,492,
269,118,276,427,117,268,484,345, 84,287, 75,196,446,247, 41,164,
14,496,119, 77,378,134,139,179,369,191,270,260,151,347,352,360,
215,187,102,462,252,146,453,111, 22, 74,161,313,175,241,400, 10,
426,323,379, 86,397,358,212,507,333,404,410,135,504,291,167,440,
321, 60,505,320, 42,341,282,417,408,213,294,431, 97,302,343,476,
114,394,170,150,277,239, 69,123,141,325, 83, 95,376,178, 46, 32,
469, 63,457,487,428, 68, 56, 20,177,363,171,181, 90,386,456,468,
24,375,100,207,109,256,409,304,346, 5,288,443,445,224, 79,214,
319,452,298, 21, 6,255,411,166, 67,136, 80,351,488,289,115,382,
188,194,201,371,393,501,116,460,486,424,405, 31, 65, 13,442, 50,
61,465,128,168, 87,441,354,328,217,261, 98,122, 33,511,274,264,
448,169,285,432,422,205,243, 92,258, 91,473,324,502,173,165, 58,
459,310,383, 70,225, 30,477,230,311,506,389,140,143, 64,437,190,
120, 0,172,272,350,292, 2,444,162,234,112,508,278,348, 76,450

# Struktura KASUMI

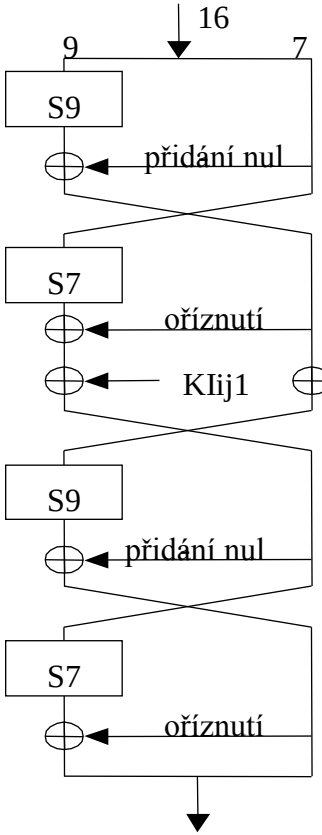
**Lehce modifikovaný algoritmus MISTY**



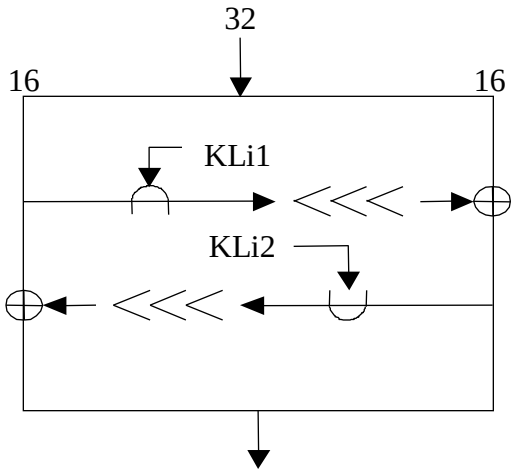

KASUMI




Funkce FO




Funkce FI




⊕ XOR
∩ AND
∪ OR
<<< rotace doleva o jeden bit

Funkce FL

# Algoritmy f1,f1*,f2,f3,f4, f5,f5*

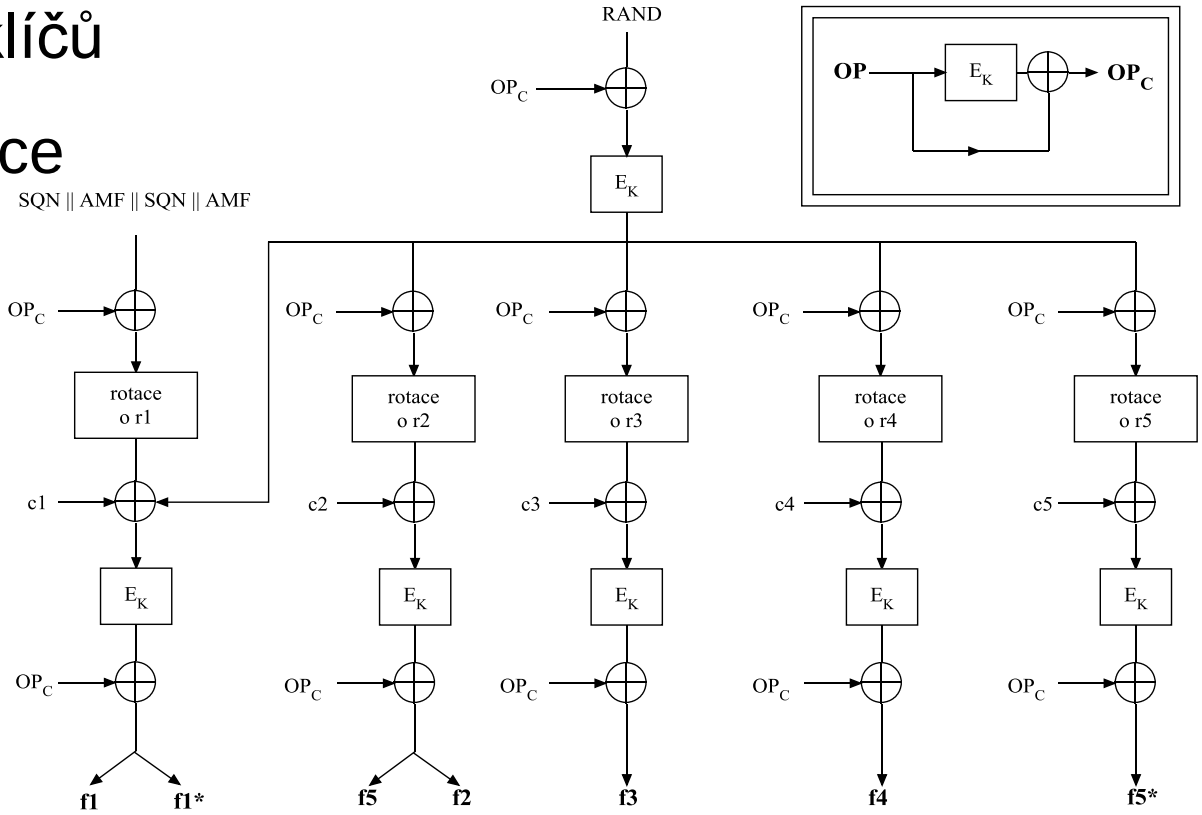
Souhrnně nazývány MILENAGE

f1,f2 – autentizace

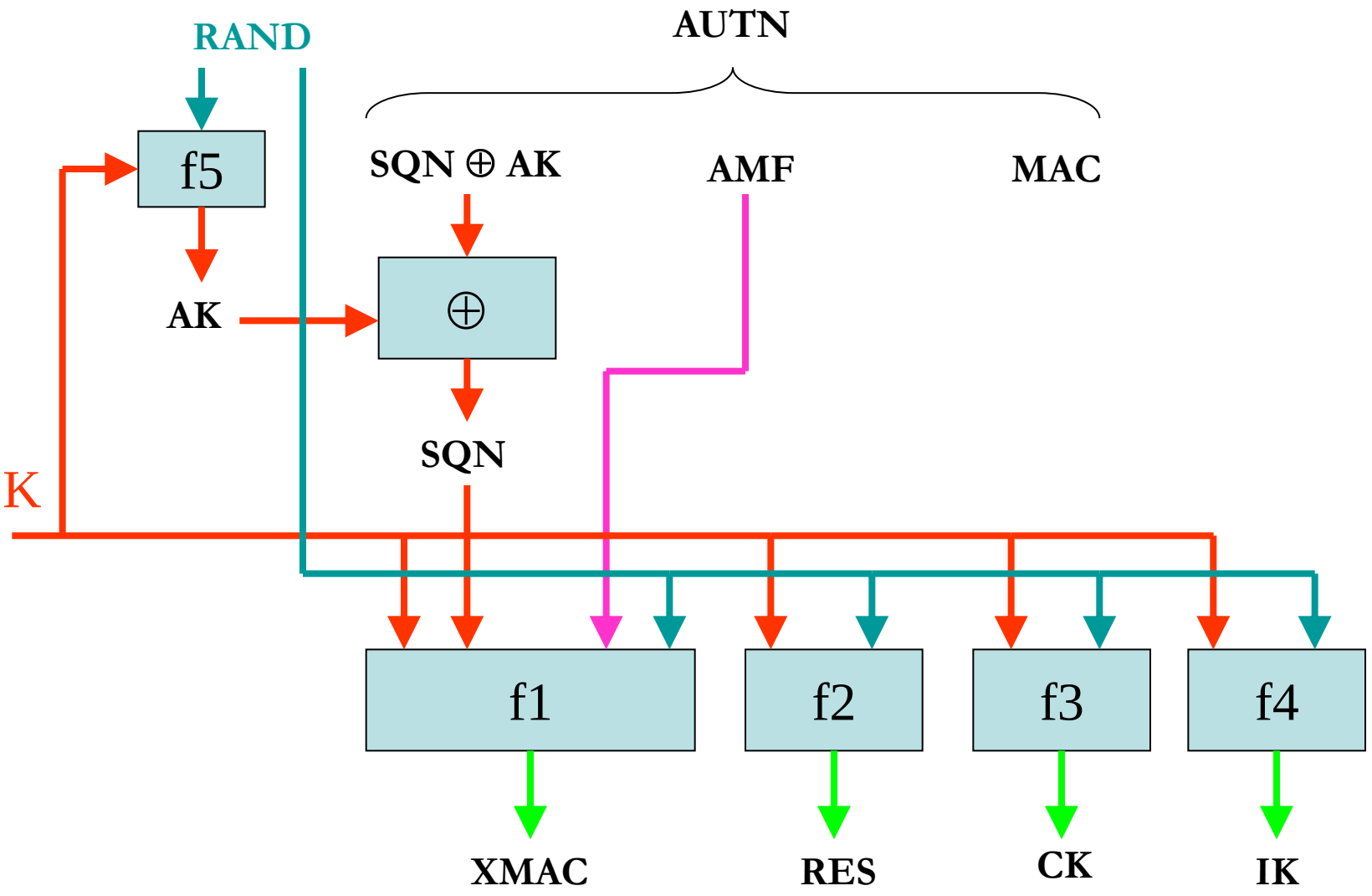
f3,f4,f5 – generování klíčů

f1*,f5* - resynchronizace

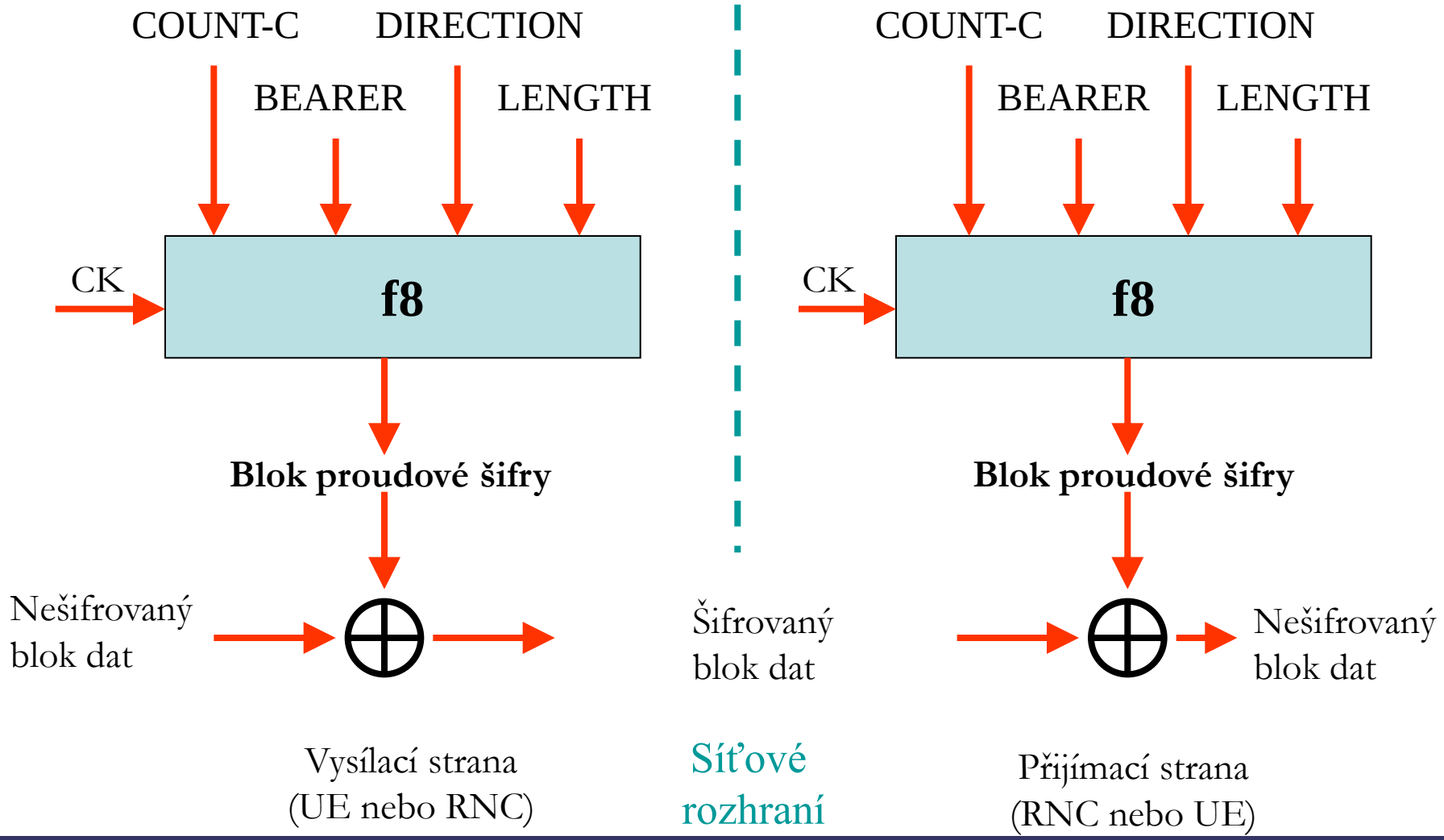
základem je Rijndael



# Šifrovací algoritmy v UMTS



# Šifrovací algoritmy v UMTS
## f8



# Šifrovací algoritmy v UMTS
## f9