Sous Systèmes Radio 2G/3G/4G
R404

IUT Béziers, dépt. R&T © 2014-2019
http://www.borelly.net/
Christophe.BORELLY@umontpellier.fr

Radio 2G

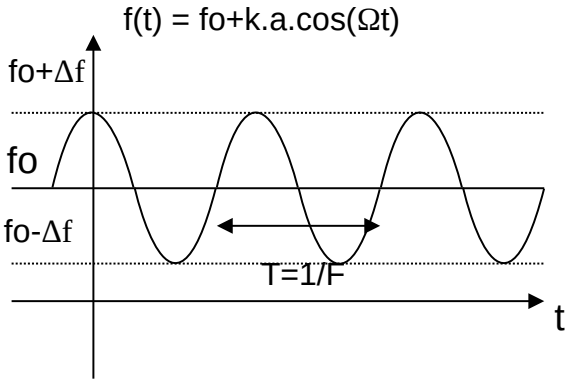
- La couche physique radio est définie dans les normes GSM 05.xx – 3GPP série 45.xx
- C'est la partie la plus complexe et sophistiquée du système GSM
- Modulation **GMSK** (270,83 Ksps)
- Largeur des canaux : 200 Khz
- Canal montant (MS-BTS) : UpLink
  - Fréquence basse (économie d'énergie)
- Canal descendant (BTS-MS) : DownLink
  - Fréquence haute

Méthodes d’accès multiple 2G

- Le système GSM combine 2 systèmes d'accès multiple.
- **FDMA** : Frequency Division Multiple Access
  - Le numéro de canal de la cellule (fréquence)
- **TDMA** : Time Division Multiple Access
  - Le numéro de slot entre 0-7 (Intervalle de temps)
- Option : saut de fréquence

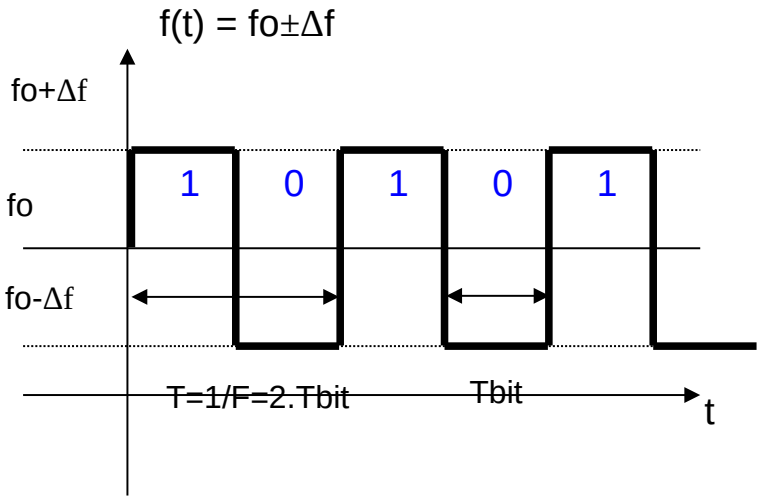
Modulation de fréquence

- Porteuse de fréquence centrale f_o
- Le signal modulant s(t)
- La fréquence instantanée du signal modulé s'écrit :
  - $f(t) = f_o + k.s(t)$
- Si s(t) est sinusoïdal, $s(t) = a.\cos(\Omega t)$
- La fréquence instantanée devient :
  - $f(t) = f_o + k.a.\cos(\Omega t)$
- L'excursion maximale en fréquence vaut :
  - $\Delta f = \pm k.a$
- L'indice de modulation m s'écrit :
  - $m = \Delta f / F$



Modulations numériques (1)

- Si le signal modulant est binaire (NRZ)
  - $f(t) = f_o \pm \Delta f$ (+ pour un “1” et – pour un “0”)



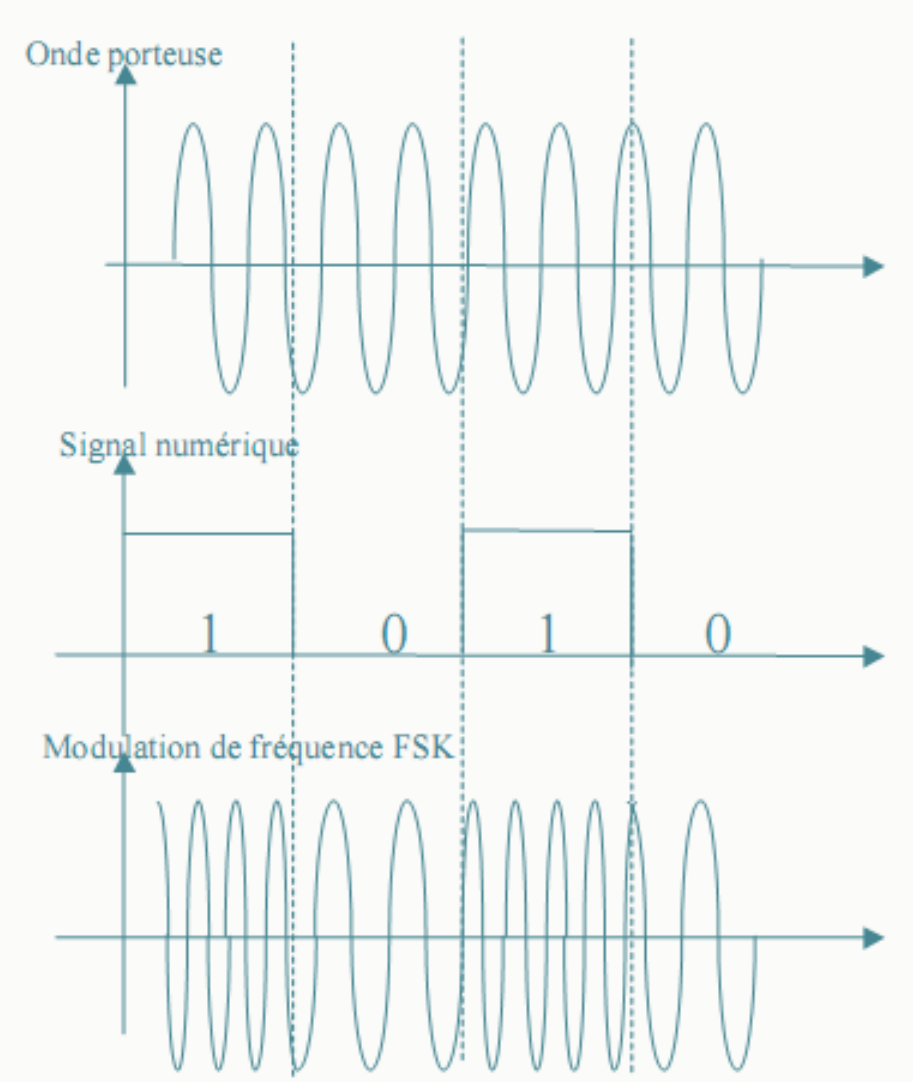
- L'intervalle de temps élémentaire (durée d'un bit) :
  - ITE = T_{bit} = 1/D, D débit binaire.

Modulations numériques (2)

- La période T=1/F est alors égale à $2.T_{bit}$.
- L'indice de modulation :
  - $m = \Delta f / F = \Delta f.2T_{bit} = 2.\Delta f / D$
- La fréquence instantanée devient :
  - $f(t) = f_o \pm \Delta f = f_o \pm mD/2$ (+ pour un “1” et – pour un “0”).
- La pulsation s'écrit
  - $w(t) = 2.\pi.f(t) = w_o \pm 2.\pi\Delta f$
- La phase (intégrale de la pulsation) est :
  - $\theta(t) = w_o t \pm 2.\pi\Delta f.t$
- la constante d'intégration est mise à zéro pour simplifier.

Modulation FSK et MSK

- Transmission d'un bit à 1
  - Sinusoïde de fréquence f0 + Δf
- Transmission d'un bit à 0
  - Sinusoïde de fréquence f0 - Δf
- Exemple : modem V23 (minitel)
  f0=1700Hz et Δf = 400Hz
  - Bit 0 -> 1300 Hz
  - Bit 1 -> 2100 Hz
- Dans le cas particulier où m=0,5, on a D=4.Δf, et 99% de la puissance du signal est contenue dans une bande de largeur 1,17.D.
- C'est la Modulation **MSK** (Minimum Shift Keying).

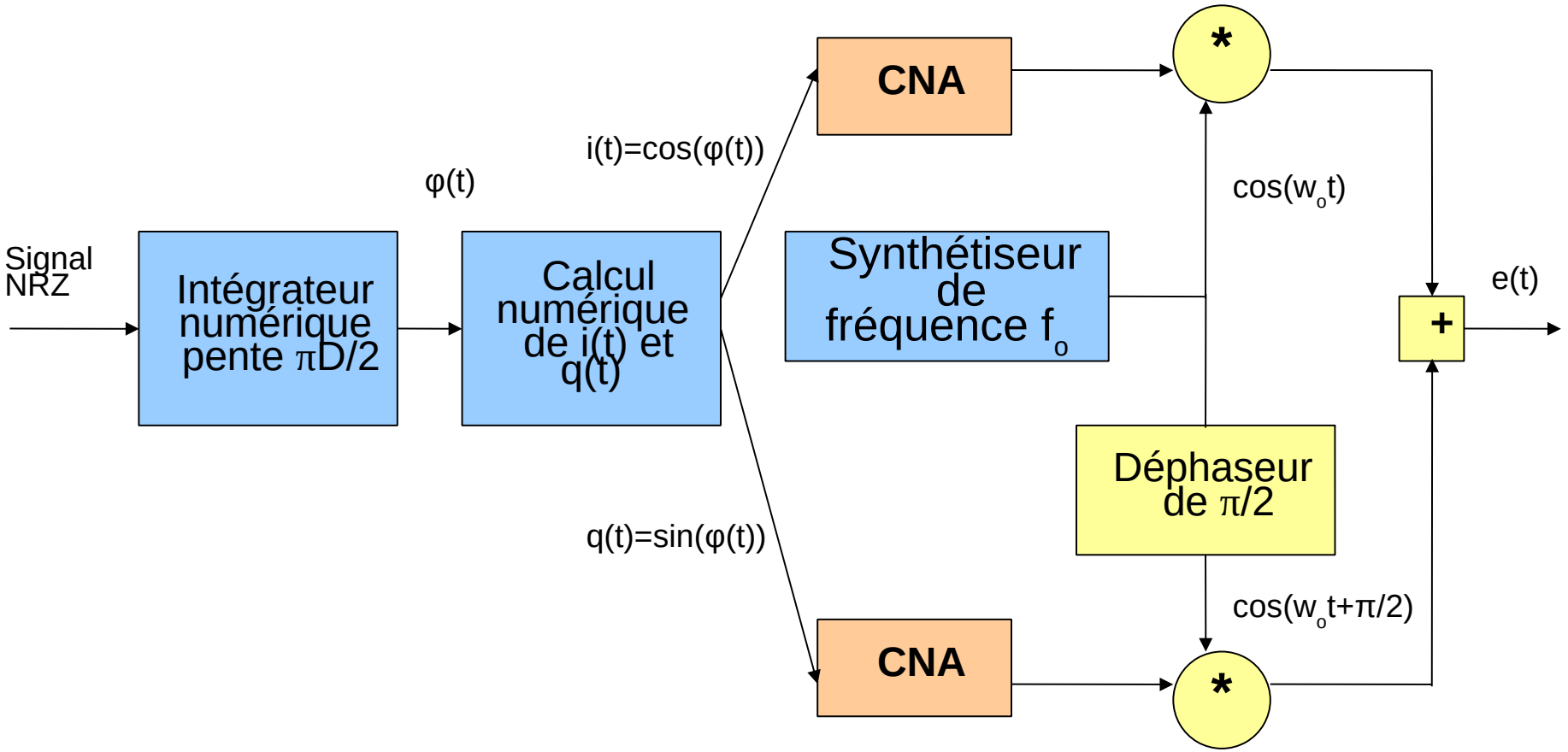


Modulateur IQ (1)

- La porteuse FSK d'amplitude normalisée (amplitude = 1) peut s'écrire :
  - $e(t)=\cos(w_o t \pm 2.\pi\Delta f.t) = \cos(w_o t + \varphi(t))$
  - $\varphi(t) = \pm 2.\pi\Delta f.t = \pm m.D.\pi.t$
  - (+ pour un “1” et – pour un “0”)
- En développant le cosinus, on obtient :
  - $e(t) = \cos(w_o t).\cos(\varphi(t)) - \sin(w_o t).\sin(\varphi(t))$
  - $e(t) = \cos(\varphi(t)).\cos(w_o t) + \sin(\varphi(t)).\cos(w_o t+\pi/2)$

Signal $i(t)$ – en phase	Signal $q(t)$ – en quadrature

Modulateur IQ (2)



Modulation GMSK

- **GMSK** : Gaussian Mimimum Shift Keying
  - Norme GSM 05.04
- Dans ce type de modulation, les données passent en premier lieu dans un filtre Gaussien.
- La fréquence de la porteuse est ensuite modulée par ce signal avec un taux de ½ (m=0,5).
- L'écart phase du signal entre deux intervalles de temps élémentaire ne dépasse pas π/2.
- L'intervalle de temps élémentaire est T = 48/16 µs, soit un débit d'environ 270,833 Ksps.

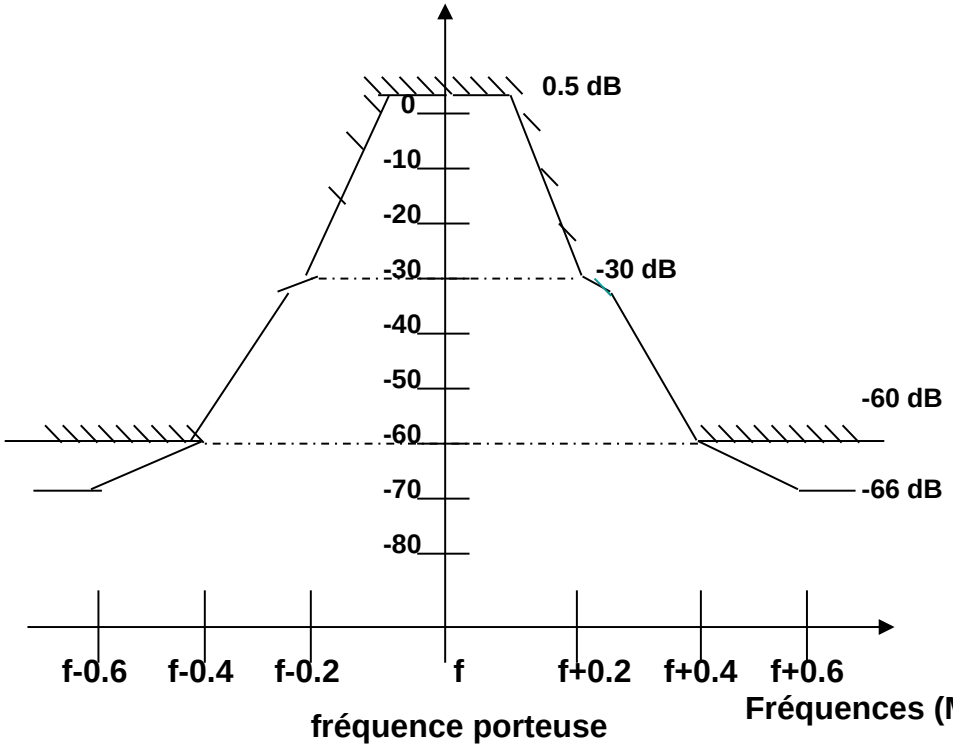
Filtre Gaussien

- Expression de la réponse impulsionnelle du filtre h(t) :
  - B.T = 0,3 et T = 48/13 µs.
  - B désigne la bande à 3 dB du filtre h(t), B = 81,25 KHz.
- Le principal intérêt de l'utilisation de cette modulation est la quasi inexistence de lobes secondaires dans la représentation spectrale.

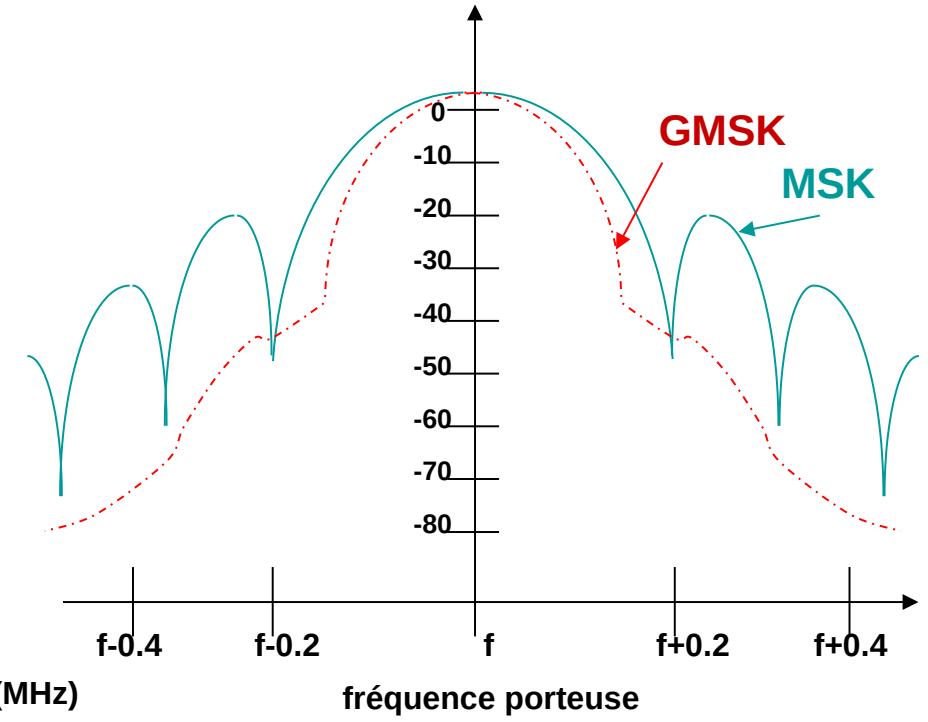
$$h(t) = \frac{1}{\lambda \cdot \sqrt{2 \cdot \pi}} \cdot \exp\left(-t^2 / \left(2\lambda^2\right)\right)$$

$$\lambda = T \cdot \frac{\sqrt{\ln(2)}}{2 \cdot \pi \cdot BT}$$

Spectre théorique GMSK



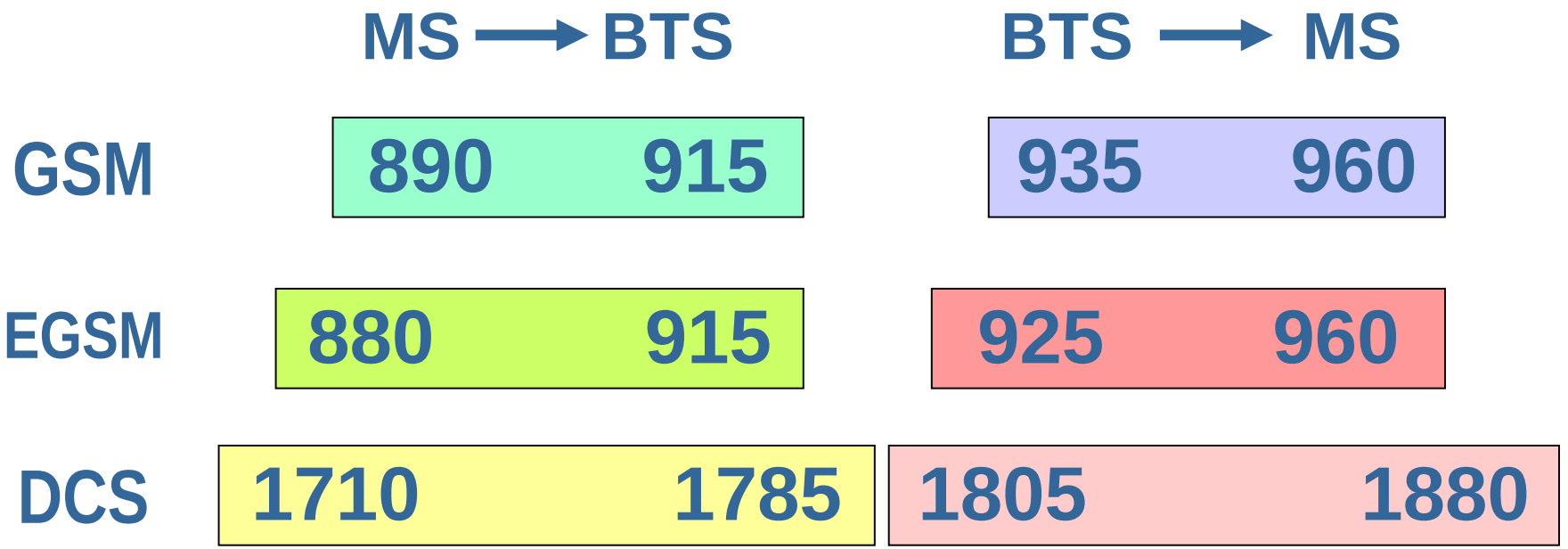
Gabarit spectral d 'un mobile GSM
(extrait de la norme GSM 05.05)



Spectre des modulations GMSK et MSK

Allocation des fréquences

- GSM 05.05 – 3GPP TS 45 005



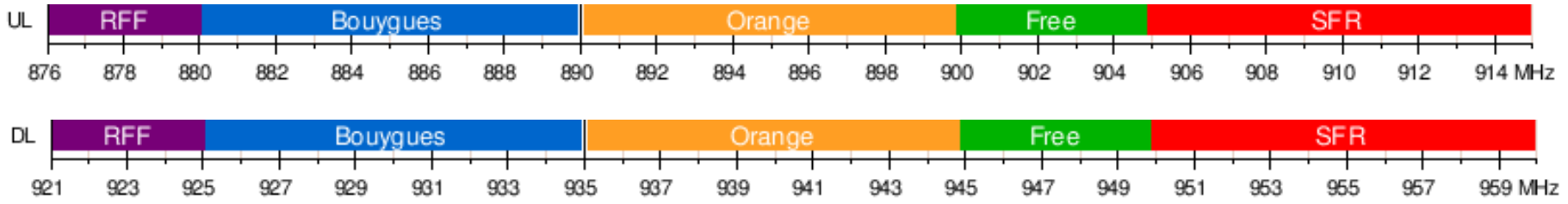
Numérotation des canaux 2G

- Largeur de 200 KHz
- 124 canaux GSM et 374 canaux en DCS.
- **ARFCN** : absolute radio frequency channel number.
- E-GSM 900 MHz
  - FL(n) = 890 + 0.2.n pour $0 \leq n \leq 124$
  - FL(n) = 890 + 0.2.(n-1024) pour $975 \leq n \leq 1\,023$
  - FU(n) = FL(n) + 45
- DCS 1 800 MHz
  - FL(n) = 1710.2 + 0.2.(n-512) pour $512 \leq n \leq 885$
  - FU(n) = FL(n) + 95

Autorité de Régulation

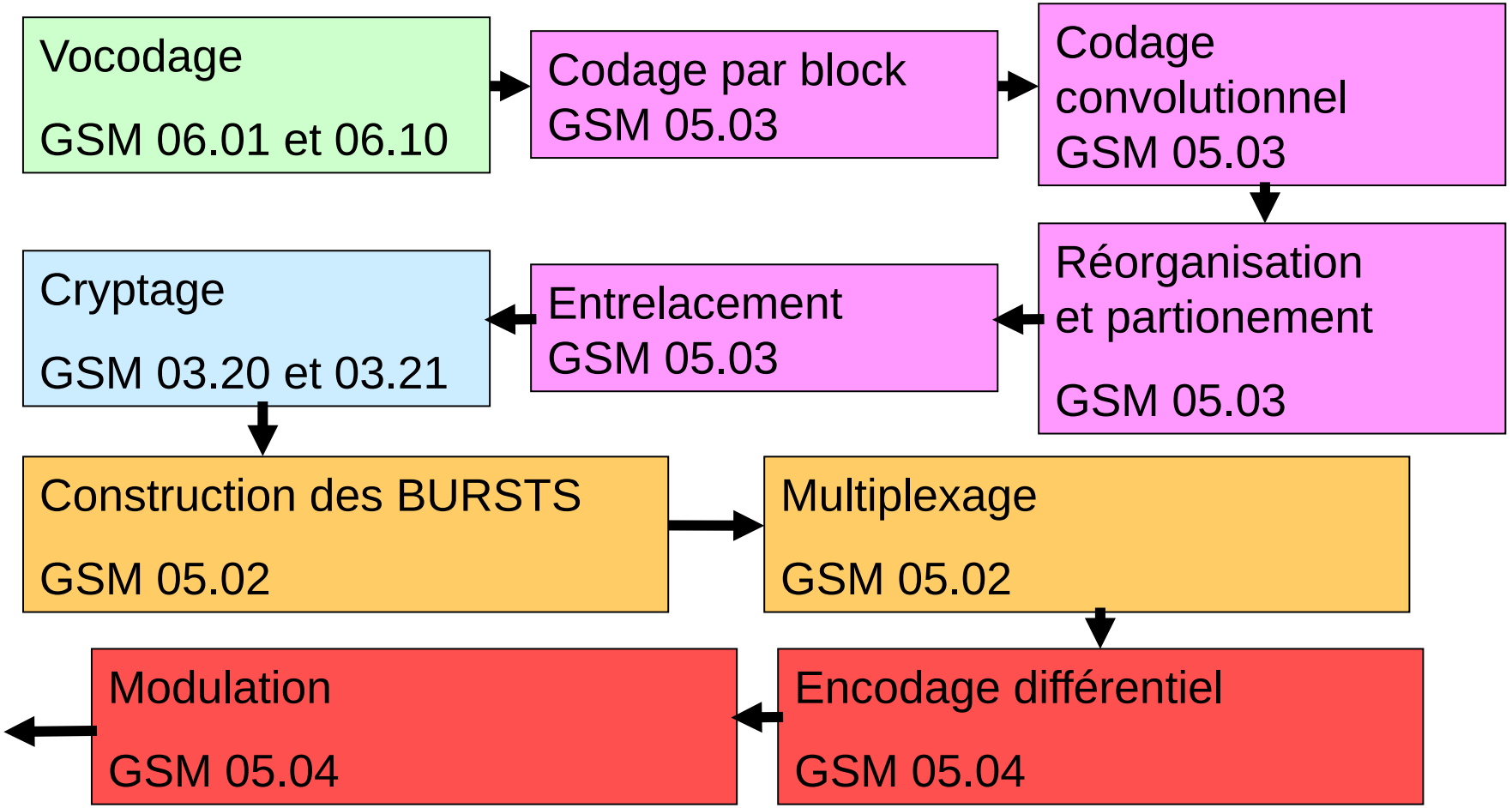
- En France, l'ARCEP (Autorité de Régulation des Communications Electriques et des Postes) gère le spectre radioélectrique :
  - http://www.arcep.fr/
- Anciennement ART (Autorité de Régulation des Télécommunications) :
  - http://www.art-telecom.fr/

Répartition 2G en France en 2013



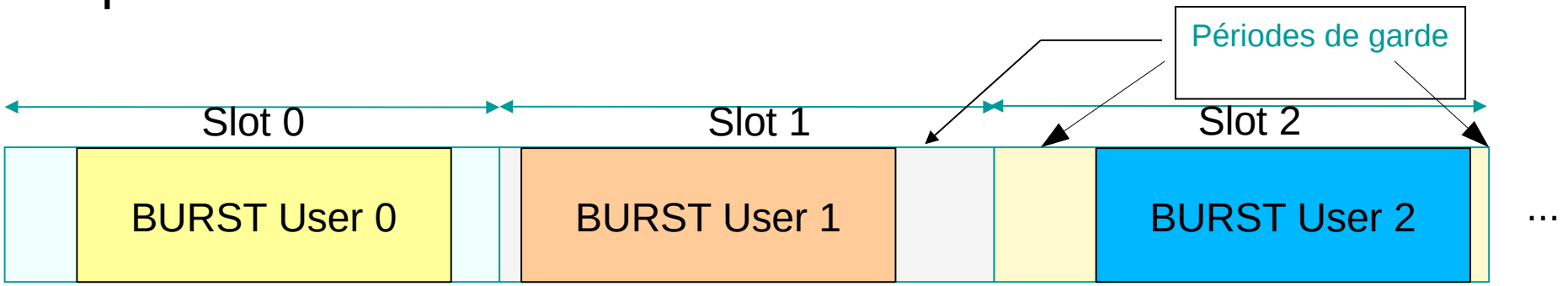
http://fr.wikipedia.org/wiki/Global_System_for_Mobile_Communications

Chaine de transmission 2G



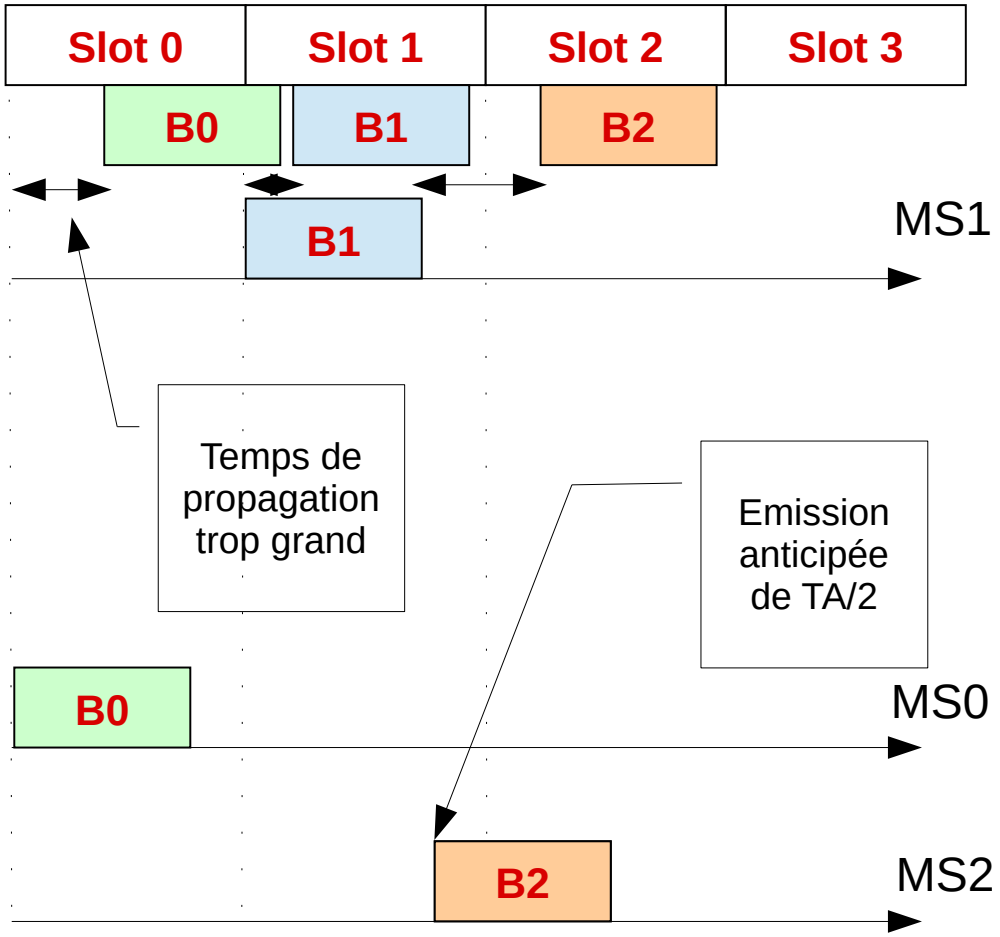
Durées élémentaires en 2G

- La durée d'un **ITE** est de T = 48/13 µs (3,692 µs)
- Le taux de modulation est d'environ 270,833 Ksps
- La modulation utilisée est de type **GMSK** (1 ITE = 1 bit)
- La ressource radio élémentaire est un **SLOT** de 156.25 ITE pour une durée de 15/26 ms (0,577 ms)
- Un slot contient un **BURST** (c.à.d. les données)
- Une période de garde de 8,25 ou 68,25 bits est utilisée pour éviter les chevauchements entre slots



Le Timing Advance (TA)

- Compenser le temps de propagation du signal (env. 30 Km en 100 µs)
- C'est pour cela que l'on a des périodes de garde
- Temps d'aller-retour entre le MS et la BTS
- Codé sur 6 bits
  - Valeurs entre 0 et 63
  - Unité en T_{ITE} (3,69 µs)

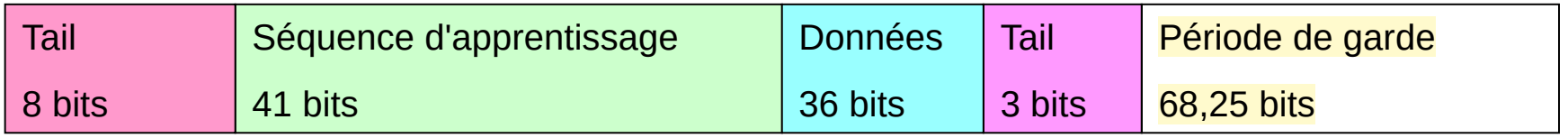


Les bursts

- Chaque slot contient un des cinq bursts possibles (cf. GSM 05.02) :
- **Burst d'accès (AB)**
  - La période de garde de 68,25 bits autorise une distance de 35 Km.
  - Ce burst est utilisé sur le RACH et après un handover.
- **Burst normal (NB)**
  - Transport des infos. Sur les canaux de trafic et de contrôle (sauf RACH).
- **Burst de synchronisation (SB)**
  - Il transporte le numéro de trame TDMA (FN) et l'identité de la BTS (BSIC).
- **Burst de correction de fréquence (FB)**
  - La répétition des FB est aussi appelé canal de correction en fréquence (FCCH).
- **Burst de bourrage (DB)**

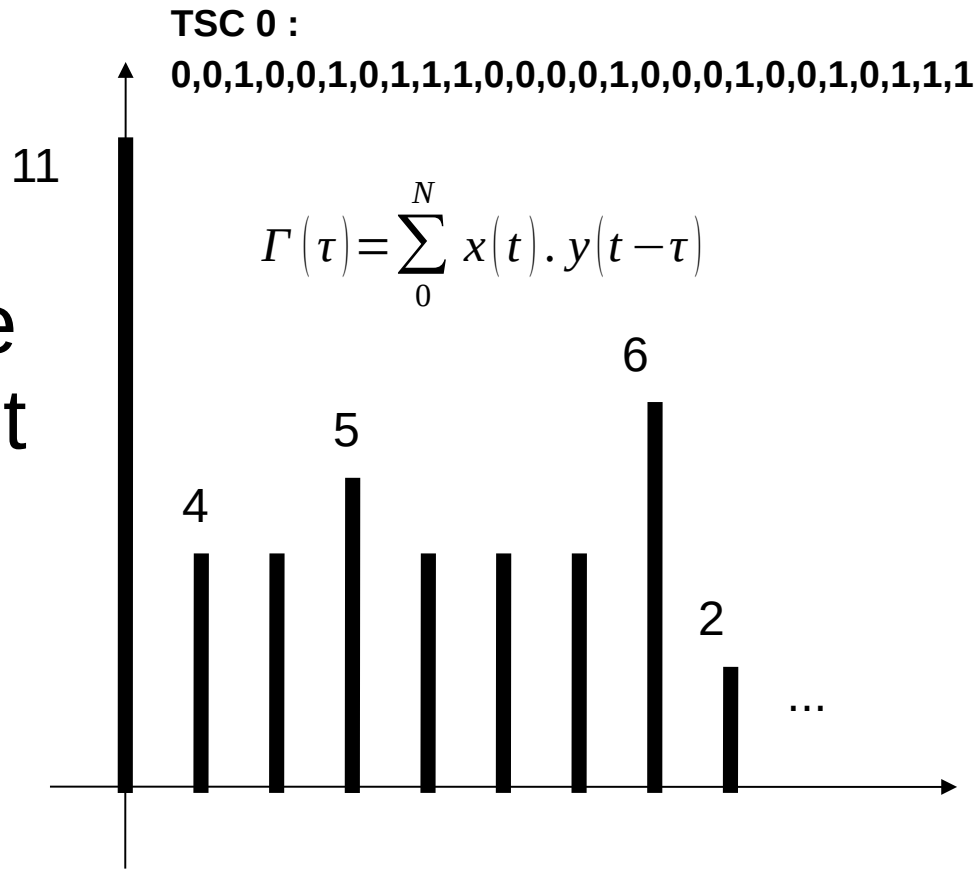
Burst d’accès (AB)

- Données : 36 bits
- Séquence d'apprentissage :
  (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1,
  1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)



Les séquences d'apprentissage

- Les séquences d'apprentissage ont des propriétés spéciales d'auto-corrélation périodique qui sont mises à profit par l'égalisateur pour déterminer précisément le début du burst



Burst normal (NB)

- Taille : 148 bits (Tail : 0,0,0)
- Données 116 bits (cf. GSM 05.03)

Tail	Données	Séquence d'apprentissage	Données	Tail	Période de garde
3 bits	58 bits	26 bits	58 bits	3 bits	8,25 bits

Training Sequence Code (TSC)	Training sequence bits (BN61, BN62 ... BN86)
0	(0,0,1,0,0,1,0,1,1,1,0,0,0,0,1,0,0,0,1,0,0,1,0,1,1,1)
1	(0,0,1,0,1,1,0,1,1,1,0,1,1,1,1,0,0,0,1,0,1,1,0,1,1,1)
2	(0,1,0,0,0,0,1,1,1,0,1,1,1,0,1,0,0,1,0,0,0,0,1,1,1,0)
3	(0,1,0,0,0,1,1,1,1,0,1,1,0,1,0,0,0,1,0,0,0,1,1,1,1,0)
4	(0,0,0,1,1,0,1,0,1,1,1,0,0,1,0,0,0,0,0,1,1,0,1,0,1,1)
5	(0,1,0,0,1,1,1,0,1,0,1,1,0,0,0,0,0,1,0,0,1,1,1,0,1,0)
6	(1,0,1,0,0,1,1,1,1,1,0,1,1,0,0,0,1,0,1,0,0,1,1,1,1,1)
7	(1,1,1,0,1,1,1,1,0,0,0,1,0,0,1,0,1,1,1,0,1,1,1,1,0,0)

Burst de synchronisation (SB)

- Données : 78 bits
- Séquence d'apprentissage étendue :
  (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0,
  0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1,
  0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)

Tail	Données	Séquence d'apprentissage	Données	Tail	Période de garde
3 bits	39 bits	64 bits	39 bits	3 bits	8,25 bits

Burst de correction de fréquence (FB)

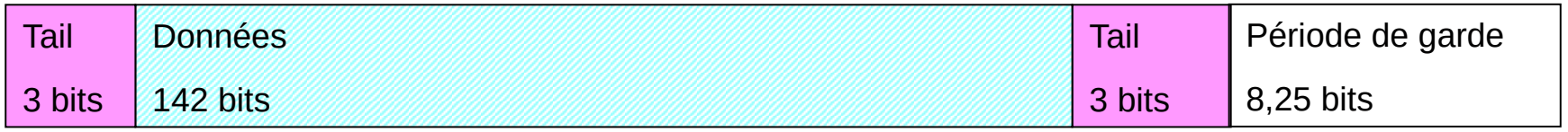
- Les données ne contiennent que des 0 soit un signal de fréquence constante f0 + 67,7 KHz (1625/24 KHz)

Tail	Données fixes	Tail	Période de garde
3 bits	142 bits	3 bits	8,25 bits

Burst de bourrage (DB)

- Les Busrts de bourrage (DB) sont utilisés pour les mesures de la qualité du lien radio.

(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1,0,
0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0,
0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0,
0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0,
0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1,
1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)

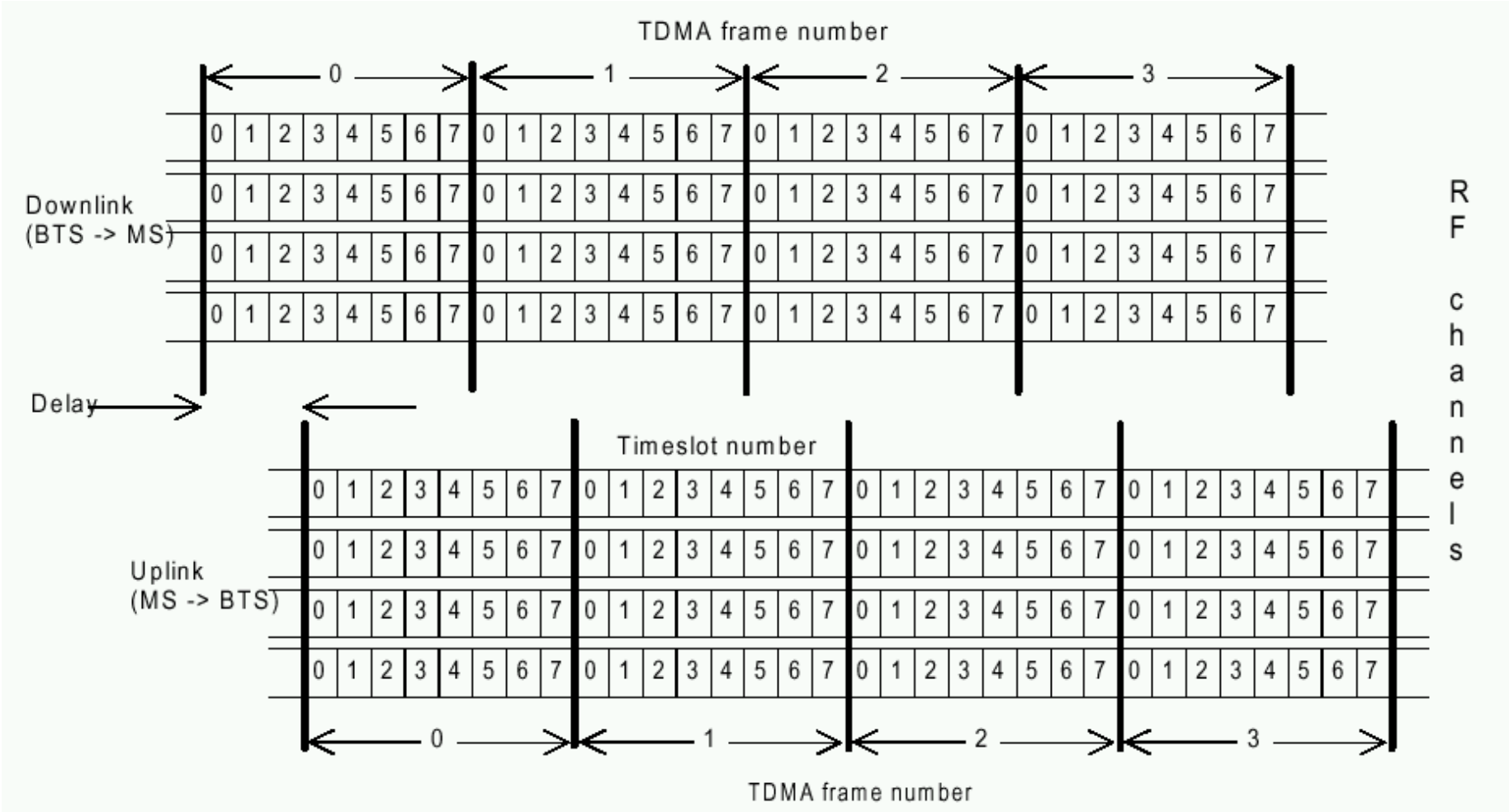


Trame TDMA

- Division en intervalles de temps IT (ou slots)
  - T_{slot} = 0,5769 ms (15/26 ms)
- Trame TDMA : Regroupement des slots par paquets de 8 :
  - $T_{TDMA} = 8.T_{slot}$ = 4,6152 ms (60/13 ms)

- Chaque utilisateur utilise 1 slot par trame TDMA
- Un «canal physique» est la répétition périodique d'un slot dans une trame TDMA sur une fréquence particulière
- Possibilité de n'allouer qu'un slot toutes les 2 trames TDMA (canal physique demi-débit pour la parole)

Times slots et TDMA frames



GSM 05.02 page 51

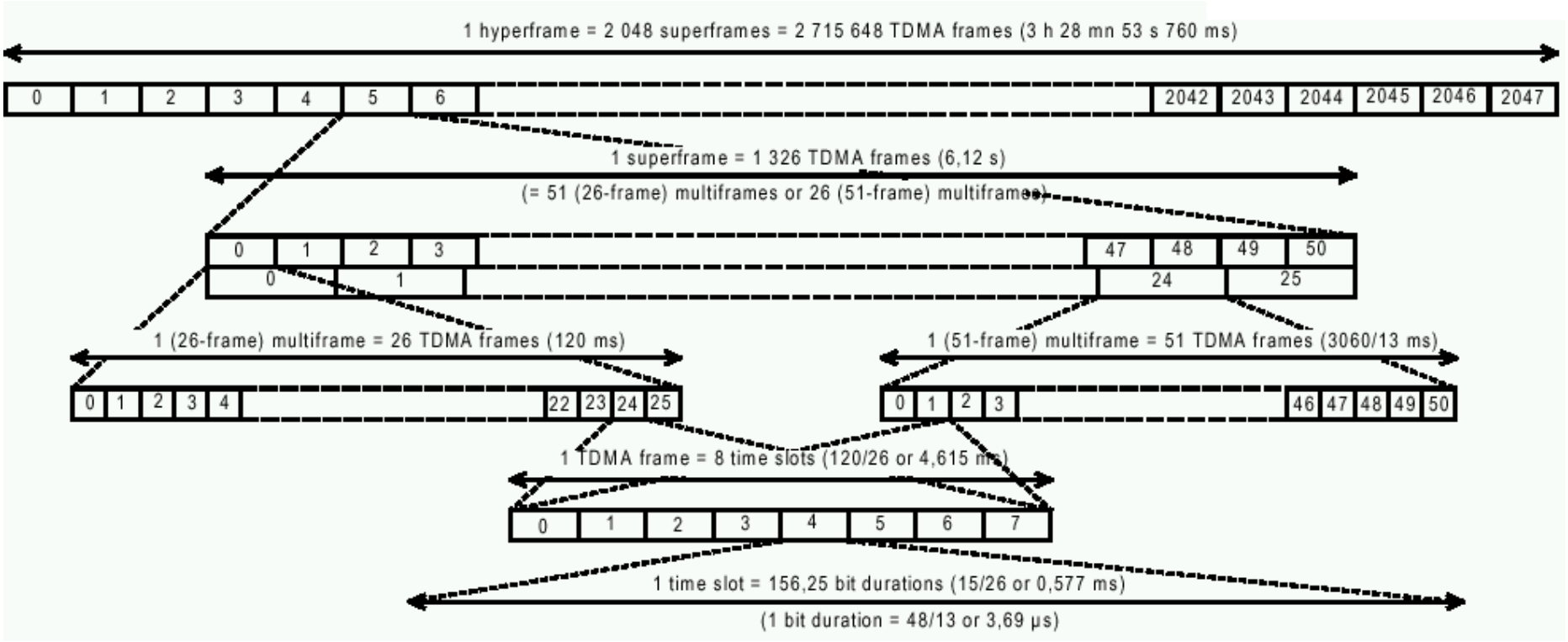
Hyper et super trames TDMA

- Les trames TDMA sont numérotées (FN)
  - 0 à 2 715 647 = 26*51*2048 -1
- La plus longue structure récurrente est une HYPER-TRAME qui dure 3 h 28 mn 53 s 760 ms (12 533,76 s)
- Chaque hyper-trame est divisée en 2 048 SUPER-TRAMES qui ont une durée de 6,12 s (1326 T_{TDMA})

Multi-trames TDMA

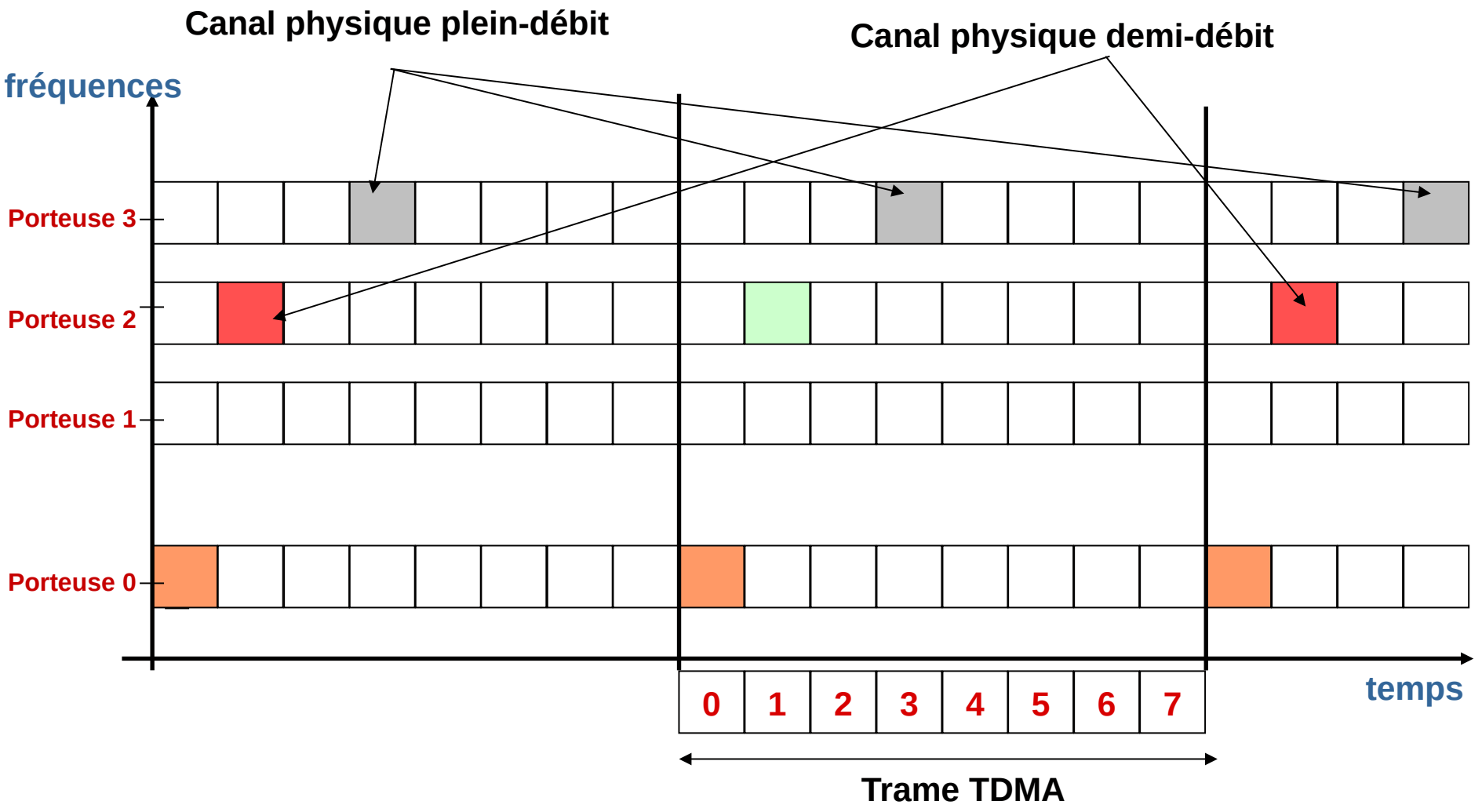
- Les super-trames sont elles même subdivisées en MULTI-TRAMES. Il y en a deux types :
  - Multi-trame 26 (51 par super-trame) d'une durée de 120 ms, qui contient 26 trames TDMA. Cette multi-trame est utilisée pour transporter les canaux TCH et SACCH
  - Multi-trame 51 (26 par super-trame) d'une durée de 235,4 ms (3 060/13 ms), qui contient 51 trames TDMA. Cette multi-trame est utilisée pour transporter les canaux BCCH, CCCH (NCH, AGCH, PCH et RACH) et SDCCH (SACCH/C)

Hyper, super, multi-trames

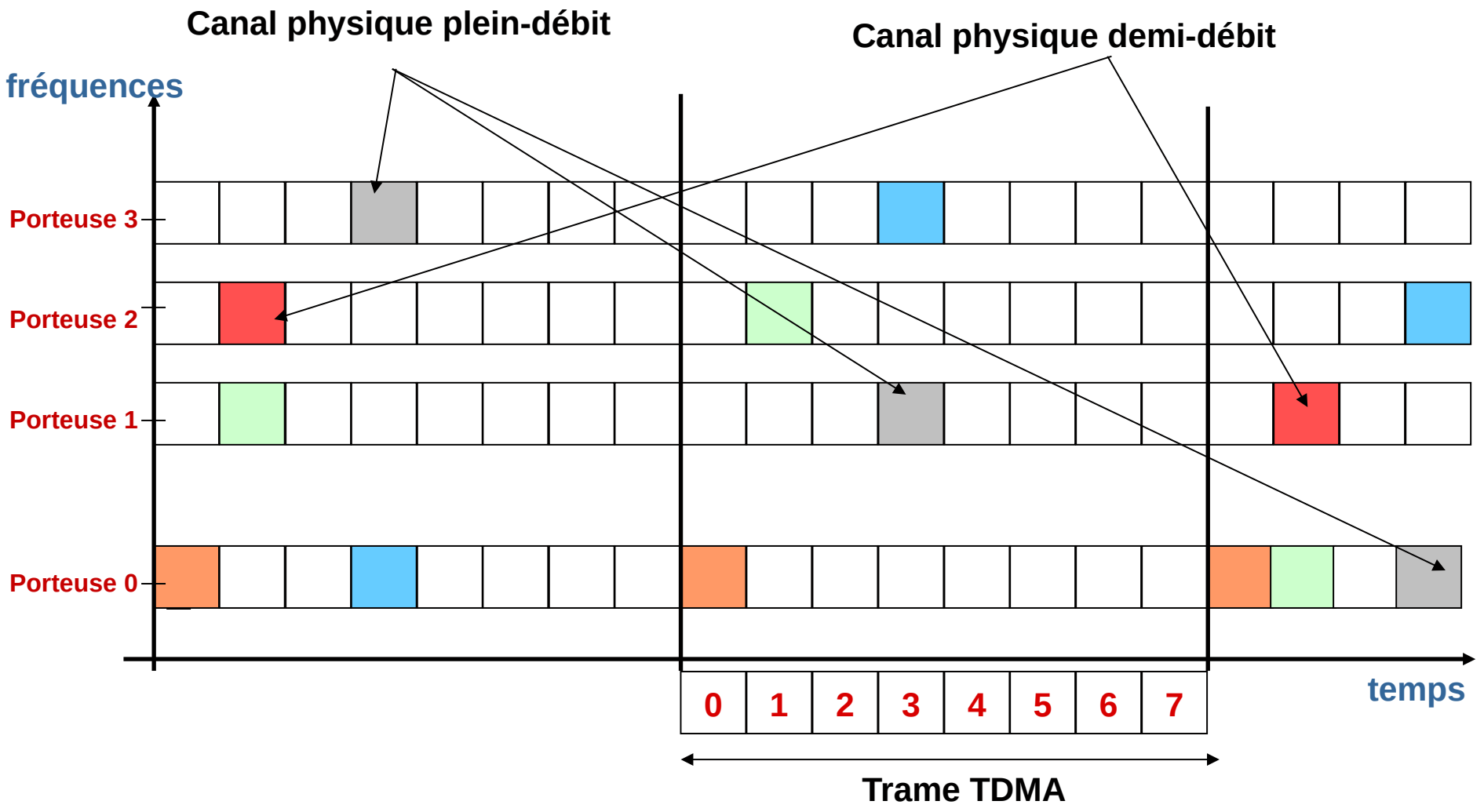


GSM 05.01 page 14

Transmission TDMA



Saut de fréquence



Les différents canaux 2G

- Numérotation :
  - Slot (TN), trame TDMA (FN), Canal RFCN
- 4 groupes de canaux :
  - **BCH** (Broadcast CHannel)
  - **CCCH** (Common Control CHannel)
  - **DCCH** (Dedicated Control CHannel)
  - **TCH** (Traffic CHannel)

Evolutions du transport de données

- La limitation du débit données pour GSM à 9.6 Kbps (TCH/F9.6) est un frein au développement des services de type Internet mobile et WAP (Wireless Application Protocol)
- Développement du réseau de données :
  - **HSCSD** : High Speed Circuit Switching Data
  - **GPRS** : General Packet Radio Service
  - **EDGE** : Enhanced Data for GSM Evolution
  - **UMTS** : Universal Mobile Telecommunication System
  - **HSPA** : High-Speed Packet Access
  - **LTE** : Long Term Evolution
  - **5G-NR** : 5G New Radio

CSD et HSCSD

- La 2G offre un débit de données de 9.6 Kbps par une technique de commutation de circuit (**CSD**, Circuit Switching Data) :
  - Réservation d'un time slot pendant la durée complète de la communication même si aucune donnée n'est transmise.
- Le système **HSD** (High Speed Data) utilise un système de codage légèrement différent qui permet d'aller jusqu'à 14.4 Kbps (cf. GSM 02.34 et GSM 03.34).
- La version **HSCSD** (High Speed Circuit Switching Data) utilise 4 time slot :
  - Soit 38.4 Kbps avec 9.6 Kbps/slot et 57.6 Kbps en HSD

GPRS

- General Packet Radio Service
  - Normes GSM 0x.6x
  - GPRS phase 1 (1997)
  - GPRS phase 2 (1999)
- Le premier déploiement date de 2002
- Le déploiement de GPRS n'est pas seulement destiné aux réseaux de type GSM
- GPRS est un système à commutation de paquets
- GPRS utilise les time slot à la demande de façon dynamique (pas de réservation permanente comme pour la voix)

Débits GPRS

- Il y a quatre schémas de codage (GSM 03.64)
- **CS-1** : 181 bits.
  - 9.05 Kbps/slot soit 72.4 Kbps/8 slots
- **CS-2** : 268 bits.
  - 13.04 Kbps/slot soit 107.2 Kbps/8 slots
- **CS-3** : 312 bits.
  - 15.6 Kbps/slot soit 124.8 Kbps/8 slots
- **CS-4** : 428 bits.
  - 21.4 Kbps/slot soit 171.2 Kbps/8 slots

Support du GPRS

- Les terminaux ne seront pas capables de traiter 8 time slot dans les deux sens du fait des coûts de traitements numérique nécessaires et de la consommation en puissance au niveau de l'émission
- La documentation technique indique le nombre de slots UL et DL
  - GPRS 3+1 : 1 TS UL et 3 TS DL
  - GPRS 4+2 : 2 TS UL et 4 TS DL

EDGE

- C’est une évolution de l’interface air
- Taux de modulation 1625/6=270,833 Kbaud.
- Modulation **8PSK** : 3 bits par symbole.
  - ITE : 812,5 Kbps (59.2 Kbps par time slot).
- EDGE Evolution (release 7) :
- Modulation **16QAM** : 4 bits par symbole.
  - ITE : 1083,3 Kbps
- Modulation **32QAM** : 5 bits par symbole.
  - ITE : 1354,2 Kbps

Débits EDGE

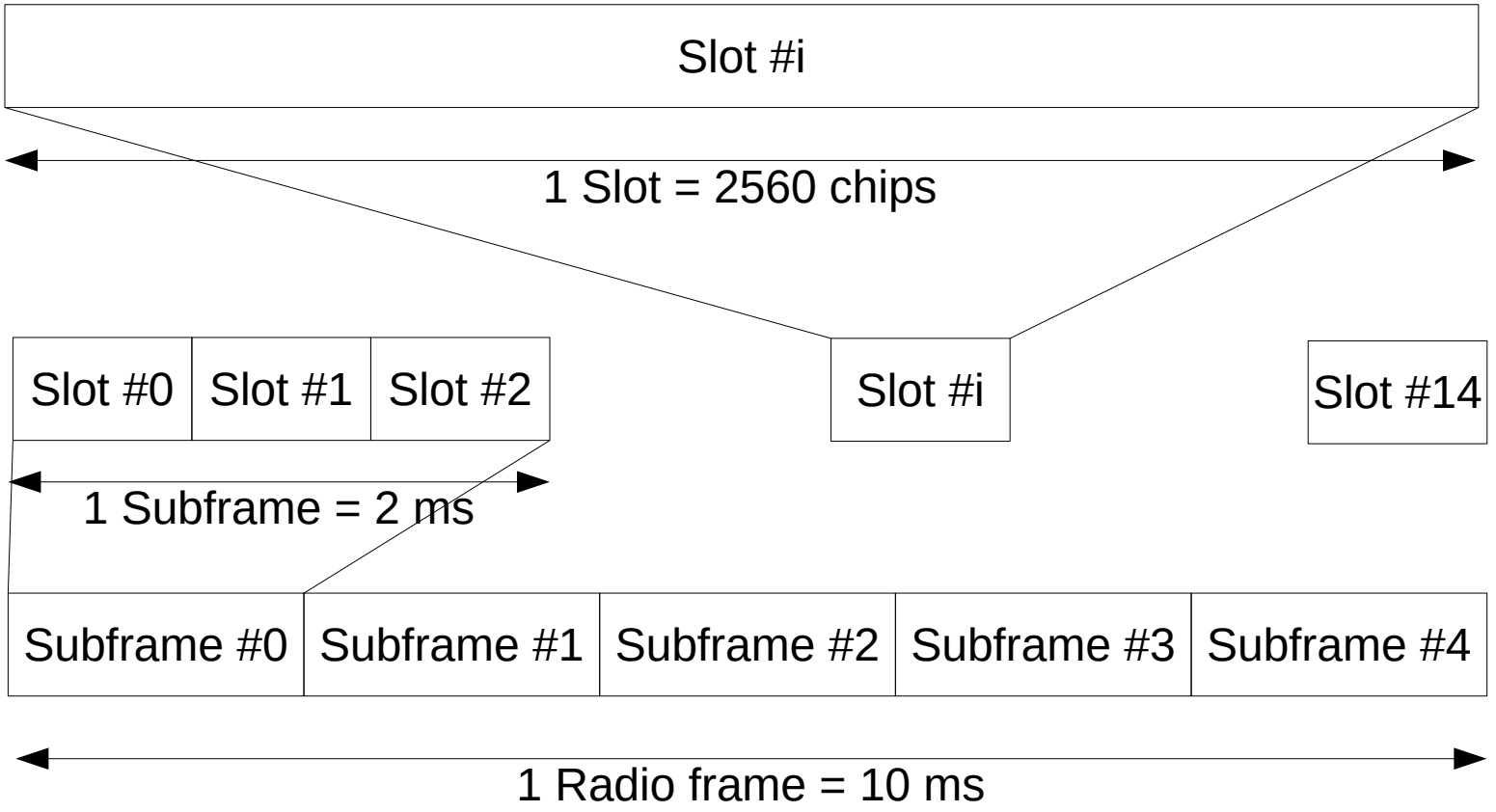
- CSD et GPRS sur EDGE sont appelés :
  - Enhanced CSD et Enhanced GPRS (05.01)

Schéma	Taux de codage	Famille	Débit (Kbps)
MCS-9	1,0	A 8PSK	59,2
MCS-8	0,92	A 8PSK	54,4
MCS-7	0,76	B 8PSK	44,8
MCS-6	0,49	A 8PSK	29,6/27,2
MCS-5	0,37	B 8PSK	22,4
MCS-4	1,0	C GMSK	17,6
MCS-3	0,85	A GMSK	14,8/13,6
MCS-2	0,66	B GMSK	11,2
MCS-1	0,53	A GMSK	8,8

Signaux radio 3G

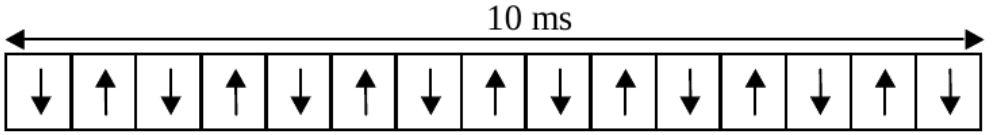
- **FDD** (TS 25.101, 25.211, 25.213)
- **TDD** (TS 25.102, 25.221, 25.223)
- Trame radio de 10 ms (15 slots)
  - Contrôle de puissance à chaque slot
- Plusieurs bandes de fréquence (26 en FDD et 8 en TDD)
  - 850MHz, 1700MHz, 1900 MHz, 2100MHz, 2500 MHz, 2600 MHz, 3500 MHz...
  - **UARFCN** : N=5*(F-Foffset) avec F en MHz
- Filtre cosinus surélevé (0,22)
- Codage canal :
  - Pas de protection
  - Codage convolutif 1/2 ou 1/3
  - Turbo code 1/3

Format des trames FDD 3GPP TS 25.211

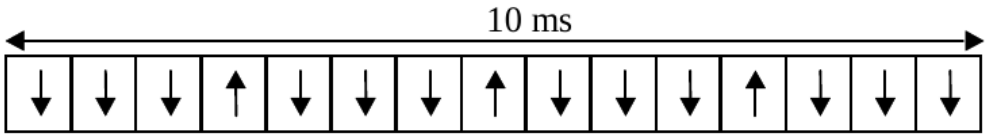


Format des trames TDD 3GPP TS 25.221

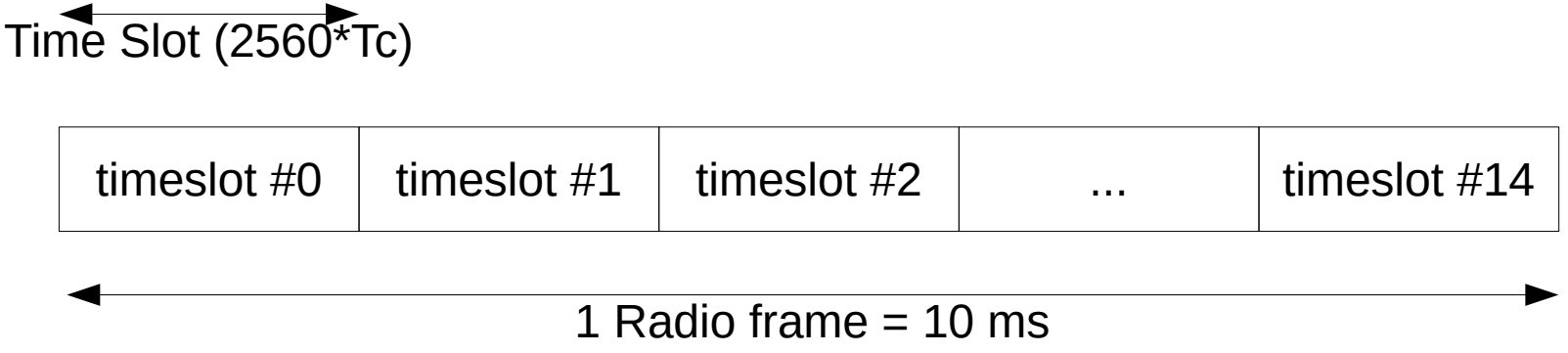
- Au moins 1 TS Downlink et 1 TS Uplink



Multiple-switching-point configuration (symmetric DL/UL allocation)



Multiple-switching-point configuration (asymmetric DL/UL allocation)



Canaux 3G

- **DCH** : Dedicated Channel (UL)
- **BCH** : Broadcast Channel (DL)
- **FACH** : Forward Access Channel (DL)
- **PCH** : Paging Channel (DL)
- **RACH** : Random Access Channel (UL)
- **USCH** : Uplink Shared Channel (UL)
- **DSCH** : Downlink Shared Channel (DL)

Canaux physiques

- **DPDCH** : Dedicated Physical Data Channel
- **DPCCH** : Dedicated Physical Control Channel
  - **TPC** : Transmit Power-Control
  - **FBI** : FeedBack Information
  - **TFCI** : Transport-Format Combination Indicator
- **S-DPCCH** : Secondary Dedicated Physical Control Channel
- **PRACH** : Physical Random Access Channel
- ...

3G FDD

- Norme 3GPP 25.213
- Accès multiple W-CDMA
- Modulation à 3,84 Mcps
- Largeur de bande 5 MHz
- **OVSF** : Orthogonal Variable Spreading Factor
  - Facteur d'étalement 256 à 4 (UL)
  - Facteur d'étalement 512 à 4 (DL)

3G TDD

- Norme 3GPP 25.223
- Accès multiple TDMA
- Modulations :
  - QPSK, 16QAM : 3,84 Mcps
    - Largeur de bande 5 MHz, SF de 1 à 16
  - QPSK, 8PSK, 16QAM : 1,28 Mcps
    - Largeur de bande 1,6 MHz, SF de 1 à 16
  - QPSK, 16QAM : 7,68 Mcps
    - Largeur de bande 10 MHz, SF de 1 à 32

Codes CDMA

- 2 types de codes sont utilisés
  - Channelisation codes et Scrambling codes
- Première étape : Channelisation (canaux)
  - Transforme chaque bit en SF chips (**SF** : Spreading Factor) : bit à 0 => +1 et bit à 1 => -1
  - Données I et Q multipliées par un code **OVSF**
- Deuxième étape : Scrambling (brouillage)
  - Appliqué au signal complexe (I+jQ)

Codes OSVF

- **OSVF** : Orthogonal Variable Spreading Factor
- Notation $C_{ch,SF,k}$
  - Numéro de canal : ch
  - Facteur d'étalement : SF (puissance de 2)
  - Numéro du code : k ($0 \leq k \leq SF-1$)
- $C_{ch,1,0}=1$

$$\begin{bmatrix} C_{ch,2,0} \\ C_{ch,2,1} \end{bmatrix} = \begin{bmatrix} C_{ch,1,0} & C_{ch,1,0} \\ C_{ch,1,0} & -C_{ch,1,0} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

FDD Uplink Scrambling codes

- Codes courts ou code longs
- Nombre de codes : 2^{24}=16777216

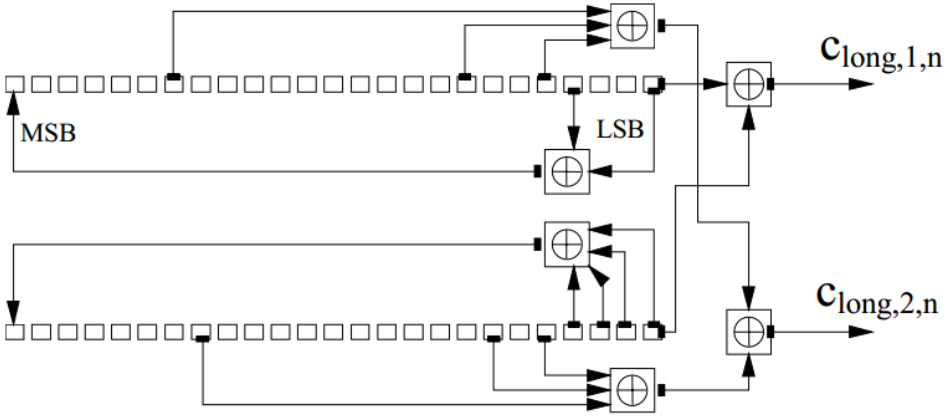


Figure 5: Configuration of uplink scrambling sequence generator

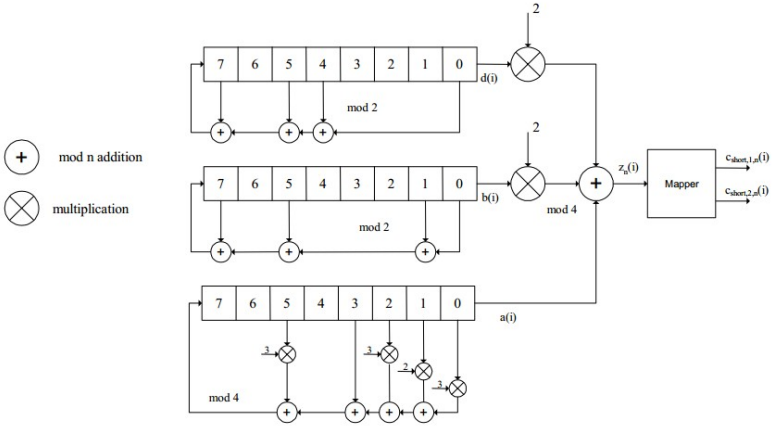
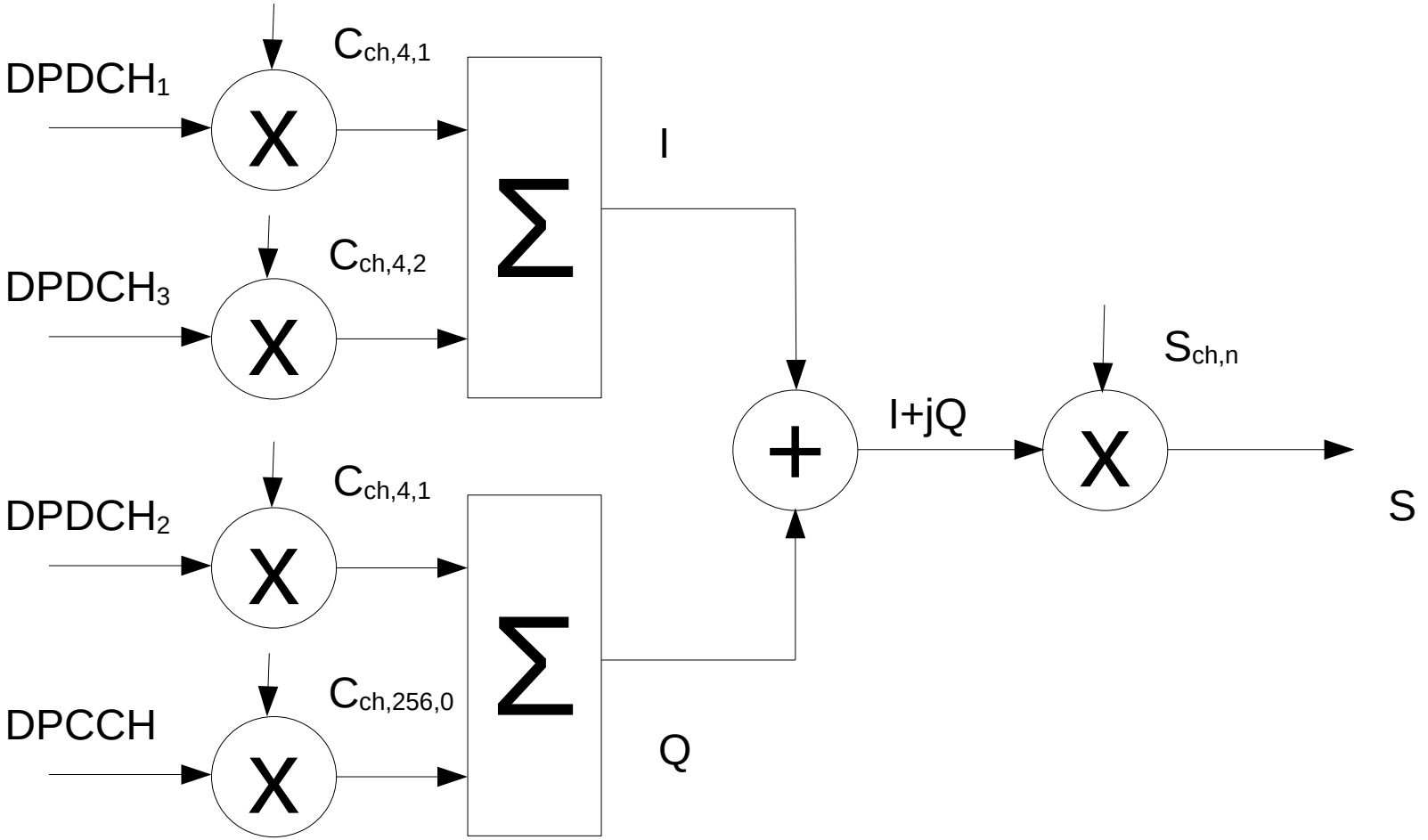
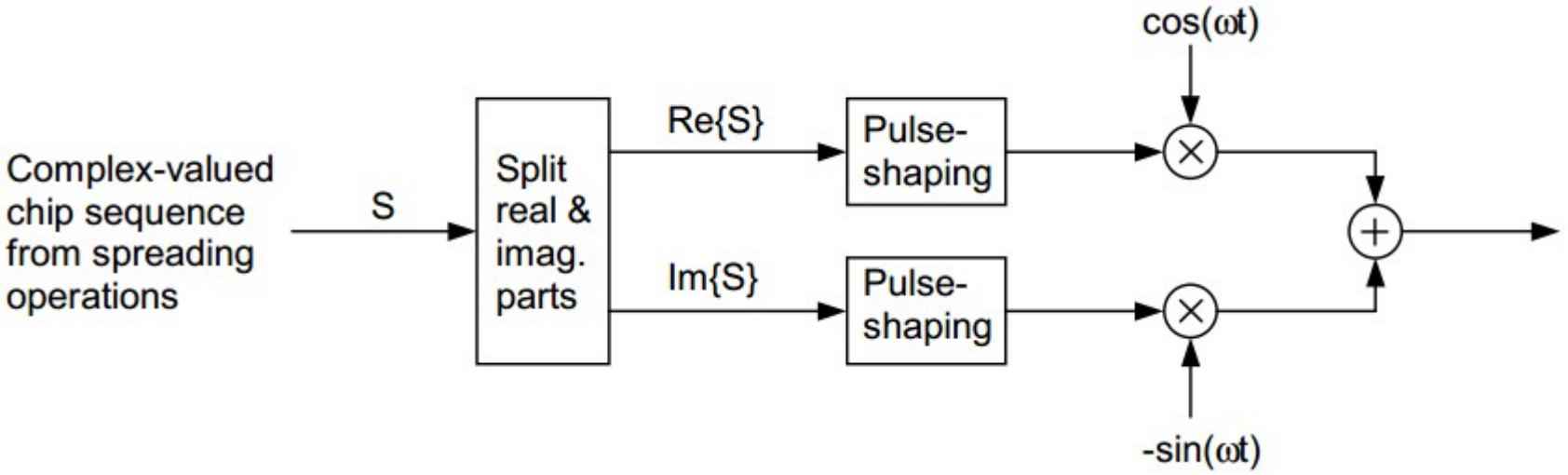


Figure 6: Uplink short scrambling sequence generator for 255 chip sequence

Exemple pour DPDCH et DPCCH



Modulation IQ



HSDPA (H)

- High-Speed Downlink Packet Access
- UMTS Release 5
- Downlink : jusqu'à 14,4 Mbps
- Uplink : 384 Kbps
- **AMC** : Adaptive Modulation and Coding
  - QPSK, 16 QAM
- **HARQ** : Hybrid automatic repeat-request
  - Redondance incrémentale (données transmisses avec plusieurs codes)
- Canal **HS-DSCH** partagé entre utilisateurs
  - HS-SCCH, HS-DPCCH et HS-PDSCH
- Ordonnancement rapide des paquets
- Mai 2007 : (102 réseau HSDPA sur 55 pays)

HARQ

- Lorsqu'un paquet reçu par le mobile est erroné, celui-ci le garde en mémoire
- A la retransmission du paquet par le réseau, la combinaison des paquets reçus permet au mobile de retrouver plus facilement les données (même si le paquet retransmis contient lui aussi des erreurs)

HSUPA (H)

- High-Speed Uplink Packet Access
- UMTS Release 6
- Downlink : jusqu'à 14,4 Mbps
- Uplink : jusqu'à 5,76 Mbps
- Ordonanceur de paquet avec le principe de « Request-Grant »
- **E-DCH** : Enhanced Dedicated CHannel (UL)
- **E-AGCH** : Access Grant Channel
- **E-RGCH** : Relative Grant Channel
- **F-DPCH** : Fractional-DPCH
- **E-HICH** : E-DCH Hybrid ARQ Indicator Channel
- **E-DPCCH** : E-DCH Dedicated Physical Control Channel
- **E-DPDCH** : E-DCH Dedicated Physical Data Channel

HSPA Evolved (H+)

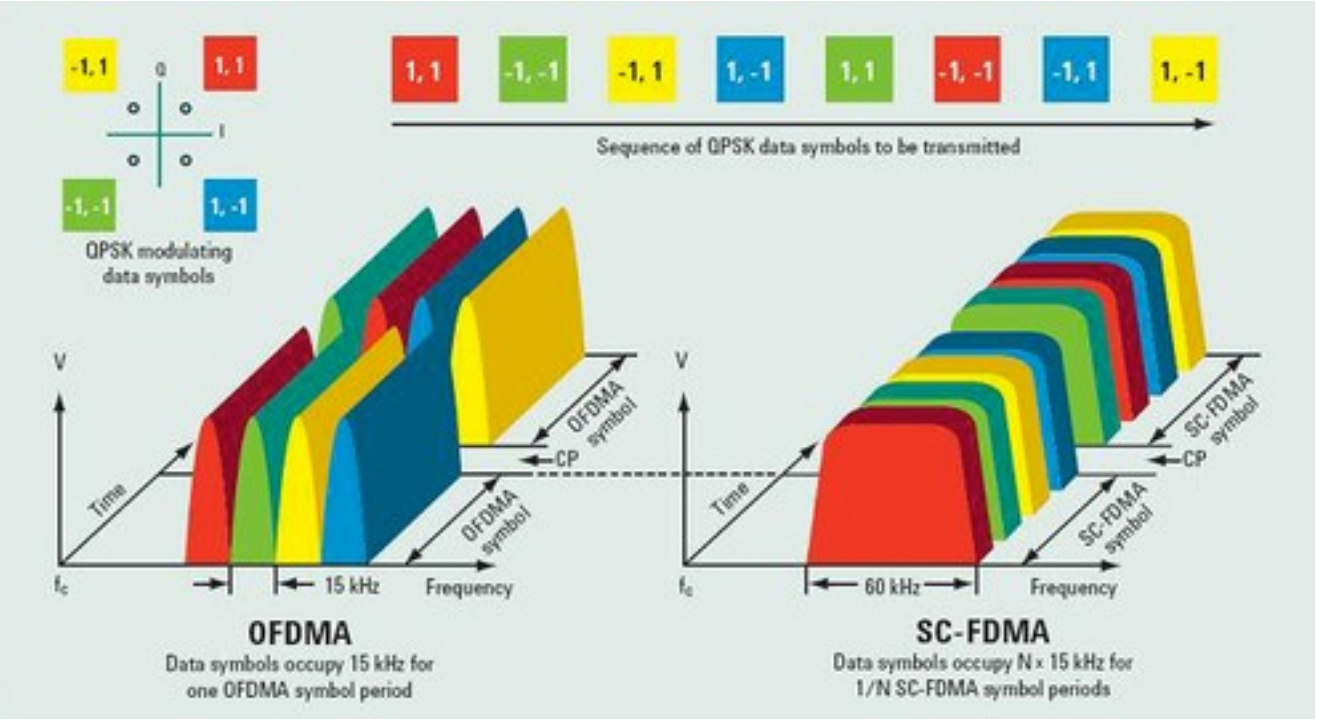
- UMTS Release 7
- Downlink : jusqu'à 42 Mbps
- Uplink : jusqu'à 11,5 Mbps
- Technologie à antennes multiples
- **MIMO** : Multiple-input multiple-output communications (MIMO 2x2)
- Beam forming (focalisation des ondes sur le récepteur)

LTE (HSOPA)

- Long Term Evolution
- High Speed OFDM Packet Access
- UMTS Release 8
- Downlink : jusqu'à 326,4 Mbps (MIMO 4x4)
- Uplink : jusqu'à 86,4 Mbps (20 MHz)
- Nouvelle « interface air »
- **OFDMA** (Downlink) et **SC-FDMA** (Uplink)
- Bande de fréquence de 1,25 à 20 Mhz
- Supporte environ 10 fois plus d'utilisateurs que W-CDMA
- Nécessite moins de puissance de calcul sur les UE.

OFDMA et SC-FDMA

- SC-FDMA (uplink) avec FFT en plus ce qui minimise PAPR (Peak-to-Average Power Ratio)



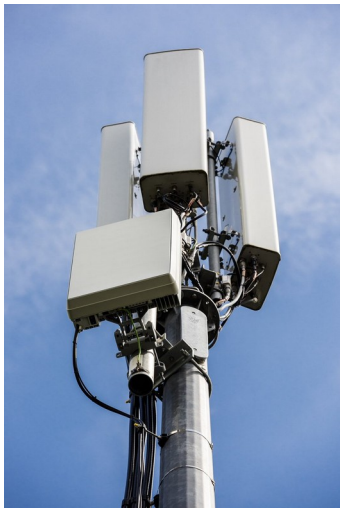
https://fr.wikipedia.org/wiki/SC-FDMA

LTE Advanced (4G)

- UMTS Release 9-10...
- Système 4G
- Downlink : jusqu'à 1Gbps (MIMO 8x8)
- Uplink : jusqu'à 500 Mbps
- Bande passante modulable jusqu'à 100 MHz
- **Carrier Aggregation** : 5 CC release 13
- **eUTRAN** (Evolved UTRAN) et eNode B
- **EPC** (Evolved Packet Core)
- VOLTE : Voice Over LTE

LTE-A Pro (4G+)

- 3GPP release 13 et 14
- Débit 3 Gbps
- 256 QAM
- 32 carrier aggregation
- Massive MIMO (plus de 64x64 antennes)
  - Double polarisation



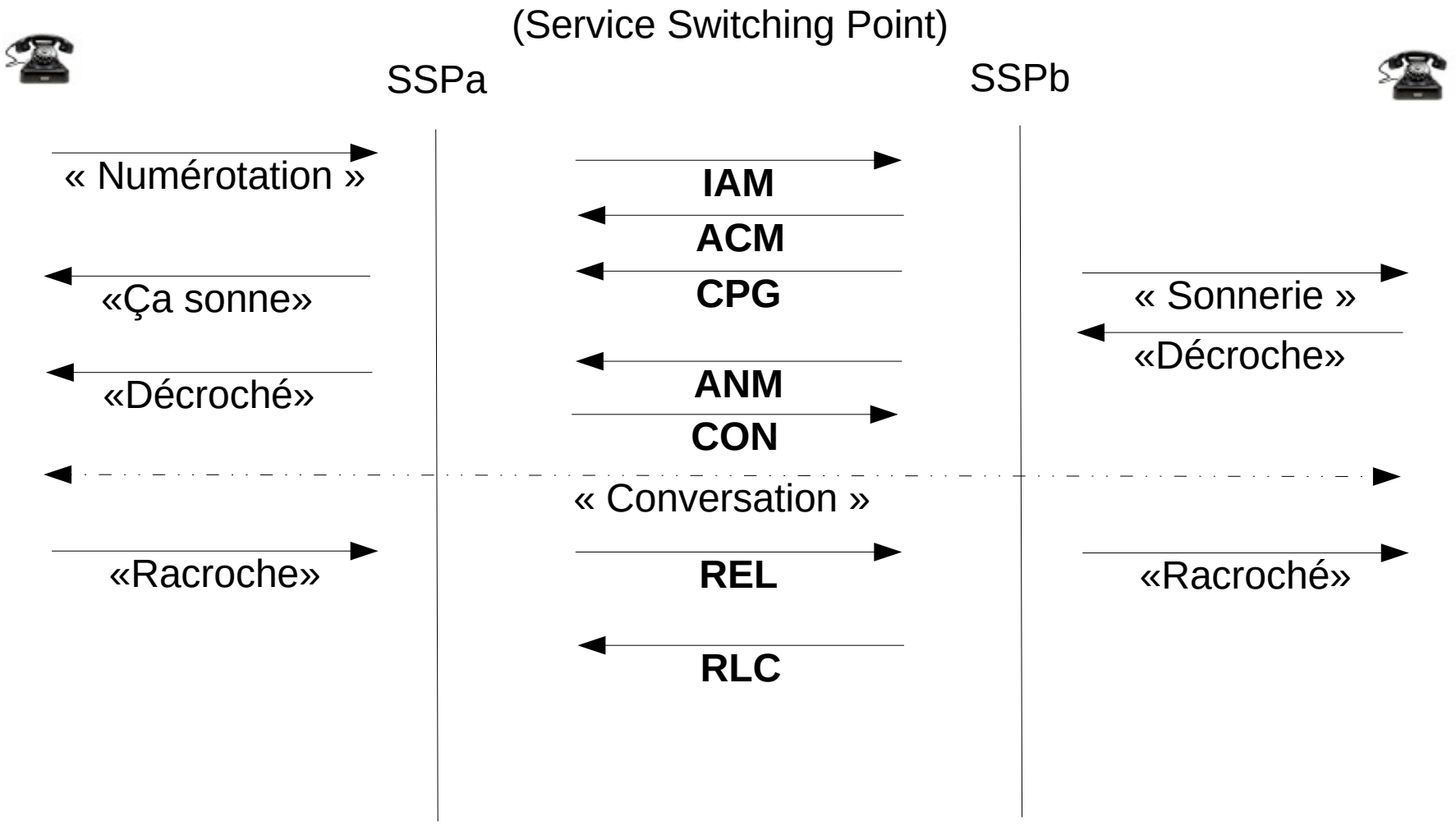
5G NR

- 3GPP TS 38.xxx - release 15 et plus
- Device to Device (D2D) communication
- Frequency Range :
  - **FR1** : En dessous de 6 GHz
  - **FR2** : 6 GHz et plus (Ondes millimétriques)
    - Portée plus faible (très atténuées : murs, précipitations)
- 3300 sous-porteuses max. sur 400 MHz
- 5 intervalles sous-porteuses :
  - 15, 30, 60, 120 et 240 Khz
  - CP (Cyclic Prefix) = 4,7 us * ($15/\Delta F_{KHz}$)
- Codage canal : **LDPC** (Low-Density Parity-Check)

Messages SS7

- **IAM** : Initial Address Message
- **ACM** : Address Complete Message
- **CPG** : Call Progress
- **ANM** : Answer message
- **CON** : Connect
- **REL** : Release
- **RLC** : Release complete

Exemple d'appel



Numérotation et identification

- Norme GSM 03.03 / 23.003
- Réseau : **MCC**, **MNC**
  - **MCC** (Mobile Country Code) : 3 digits
  - **MNC** (Mobile Network Code) : 2 digits
- Cellule : LAI, RAI, CGI, BSIC
- Mobile : IMSI, TMSI, MSISDN, MSRN

Bulletin d'exploitation de l'UIT

- **UIT** : Union internationale des télécommunications
  - Orange France 208 01
  - Orange France 208 02
  - MobiquiThings 208 03
  - Sisteer 208 04
  - Globalstar Europe 208 05
  - Globalstar Europe 208 06
  - Globalstar Europe 208 07
  - S.F.R. 208 09
  - S.F.R. 208 10
  - S.F.R. 208 11
  - S.F.R. 208 13
  - RFF 208 14
  - Free Mobile 208 15
  - Bouygues Telecom 208 20
  - Bouygues Telecom 208 21
  - ...

Identifiants

- Zone de localisation
  - **LAI** = MCC + MNC + LAC (2 octets)
- Zone de routage
  - **RAI** = LAI + RAC (1 octet)
- Numéro de cellule
  - **CGI** = LAI + CI (2 octets)
- Numéro de station de base
  - **BSIC** = NCC + BCC
    - Network Color Code : 3 bits
    - Base station Color Code : 3 bits

Identification du mobile

- **IMSI** (International Mobile Subscriber Identity)
  - MCC (Mobile Country Code) : 3 digits
  - MNC (Mobile Network Code) : 2 digits
  - MSIN (Mobile Subscriber Identification Number) max. 10 digits
- **MSISDN** (Mobile Station International ISDN Number) : Numéro de l'abonné
- **MSRN** (Mobile Station Roaming Number) : Numéro utilisé lors d'un routage inter-opérateurs

TMSI

- L'IMSI est connu uniquement à l'intérieur du réseau mobile, cette identité doit rester secrète autant que possible (recours au TMSI)
- Le **TMSI** (Temporary Subscriber Identification Number) est alloué temporairement par un VLR lors de la mise à jour de localisation ou lors de l'inscription du mobile sur le réseau
- Il est codé sur 4 octets

Recherche d'un mobile

- Lorsqu'un appel entrant se produit, le réseau va rechercher le mobile dans la dernière zone de localisation connue (plusieurs cellules)
- Messages de paging (couche 3) contenant en général le TMSI du mobile (PAGING REQUEST/RESPONSE)

La couche 3 (MS-BTS)

- Interface **Um** (GSM 04.08)
- 3 sous couches
  - **RR** : Radio Ressource
  - **MM** : Mobility Management
  - **CM** : Connection Management

TI/SI 4 bits	Protocol Discriminator 4 bits
Message Type 8 bits	
...	

0011 Call Control messages
0101 Mobility Management messages
0110 Radio Resource management messages

Exemple Paging

- 06 21 00 05 f4 a5 02 21 49
- 06 27 01 03 23 58 01 05 f4 a5 02 21 49
- Couche RR (06)

```
0 0 1 0 0 - - -  Paging messages:
          0 0 1  - PAGING REQUEST TYPE 1
          0 1 0  - PAGING REQUEST TYPE 2
          1 0 0  - PAGING REQUEST TYPE 3
          1 1 1  - PAGING RESPONSE
```

Table 10.1/GSM 04.08 (page 1 of 2)
Message types for Radio Resource management

Contenu du message

- 06 21 00 05 f4 a5 02 21 49

IEI	Information element	Type / Reference	Presence	Format	length
	L2 Pseudo Length	L2 Pseudo Length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	½
	Skip Indicator	Skip Indicator 10.3.1	M	V	½
	Paging Request Type 1 Message Type	Message Type 10.4	M	V	1
	Page Mode	Page Mode 10.5.2.26	M	V	½
	Channels Needed for Mobiles 1 and 2	Channel Needed 10.5.2.8	M	V	½
→	Mobile Identity 1	Mobile Identity 10.5.1.4	M	LV	2-9
17	Mobile Identity 2	Mobile Identity 10.5.1.4	O	TLV	3-10
	P1 Rest Octets	P1 Rest Octets 10.5.2.23	M	V	0-17

Table 9.22/GSM 04.08
PAGING REQUEST TYPE 1 message content

Codage de l'identité du mobile

- 10.5.1.4 Mobile identity
  - 05 f4 a5 02 21 49

Longueur 8 bits		
Digit 1 4 bits	Ind. 1 bit	Type 3 bits
Digit p+1 4 bits	Digit p 4 bits	
...		

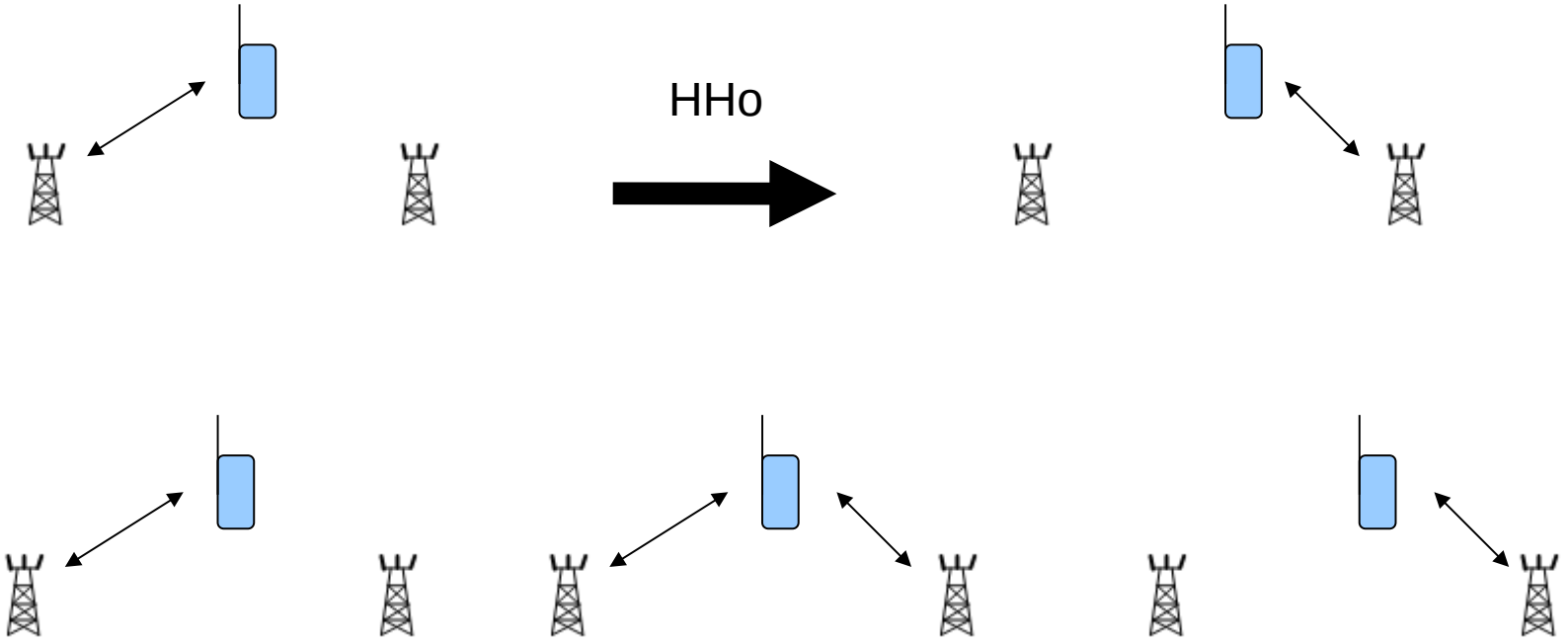
001 IMSI
010 IMEI
011 IMEISV
100 TMSI
000 No identity

If the mobile identity is the TMSI then bits 5 to 8 of octet 2 are coded as '1111' and bit 8 of octet 3 is the most significant bit.

Handover

- Si au cours du déplacement d'un MS, le signal reçu de la cellule serveuse est plus faible que sur une cellule voisine, le réseau peut demander au mobile de changer de cellule serveuse.
- Cette opération porte le nom de Handover ou Handoff suivants les systèmes.
  - Hard Handover : commutation directe
  - Soft Handover : commutation avec 2 liaisons simultanées

Hard et Soft Handover

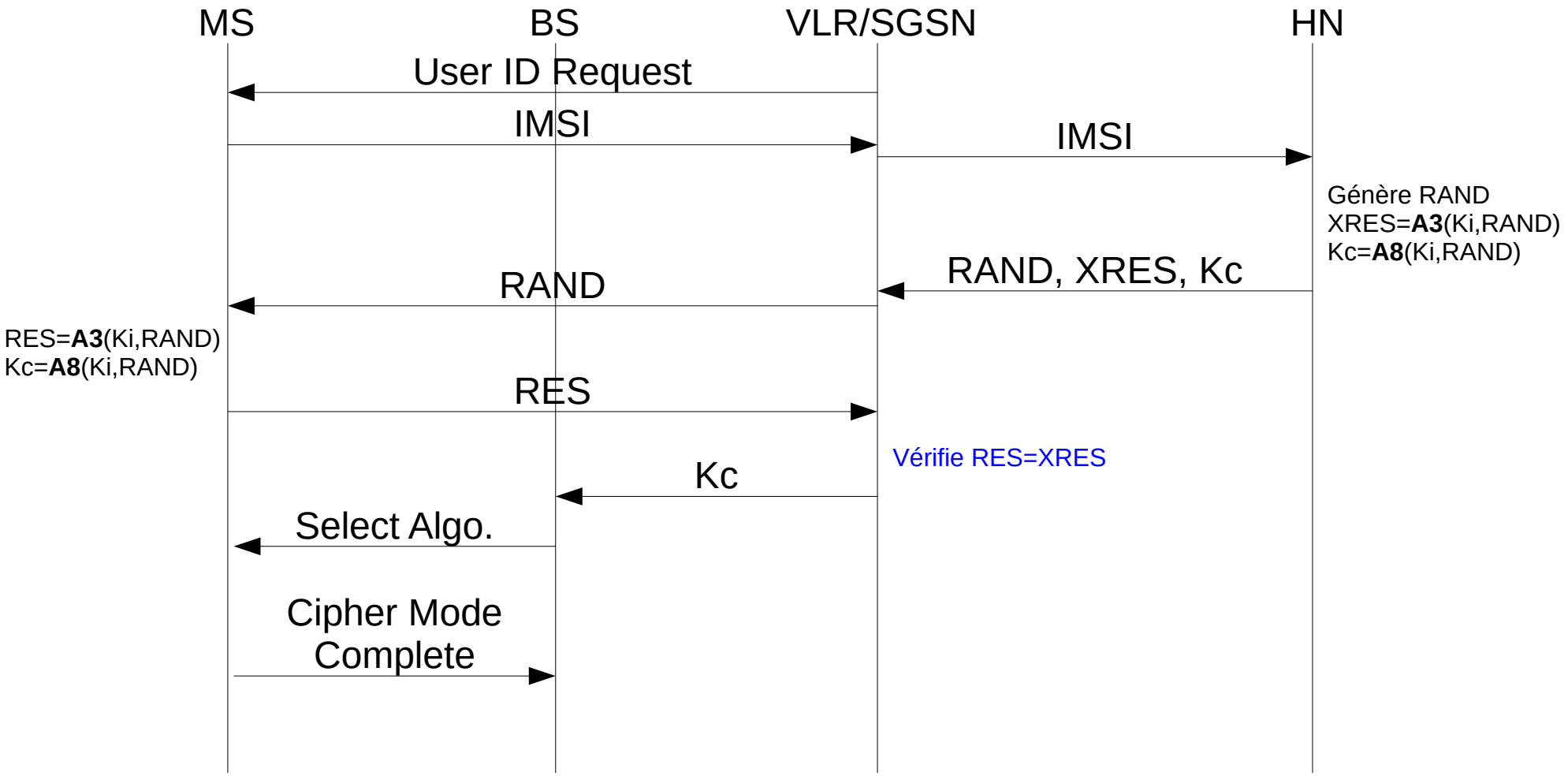


SHo : 2 Liaisons simultanées

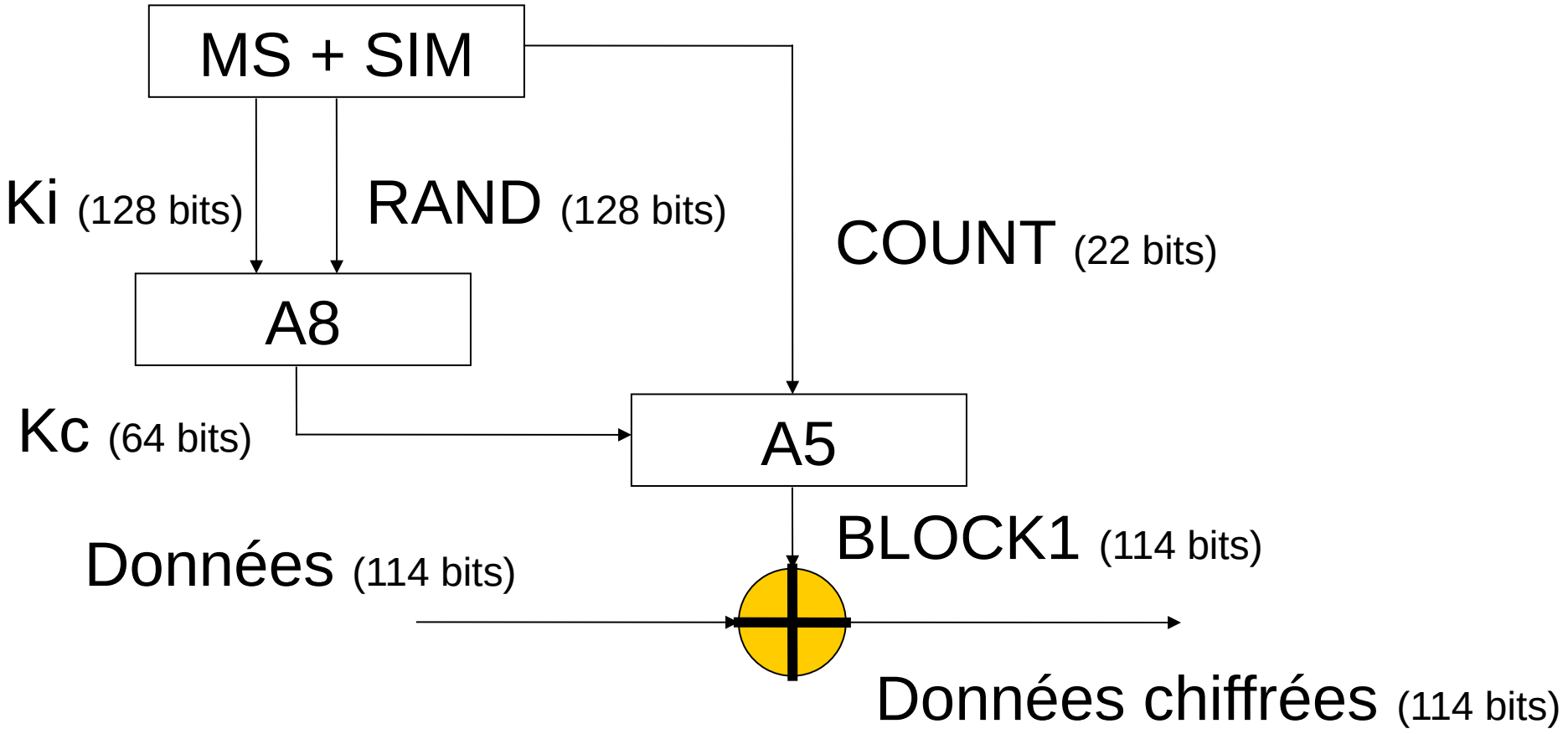
Sécurité 2G

- Utilisation de 3 algorithmes (A3, A5 et A8)
- Authentification du MS uniquement
  - Vérification de **Ki** (Clé utilisateur – 128 bits)
- Chiffrement par XOR des données
  - **Kc** (Clé de chiffrement - 64 bits)

Authentification 2G



Le chiffrement 2G



Sécurité 3G/4G

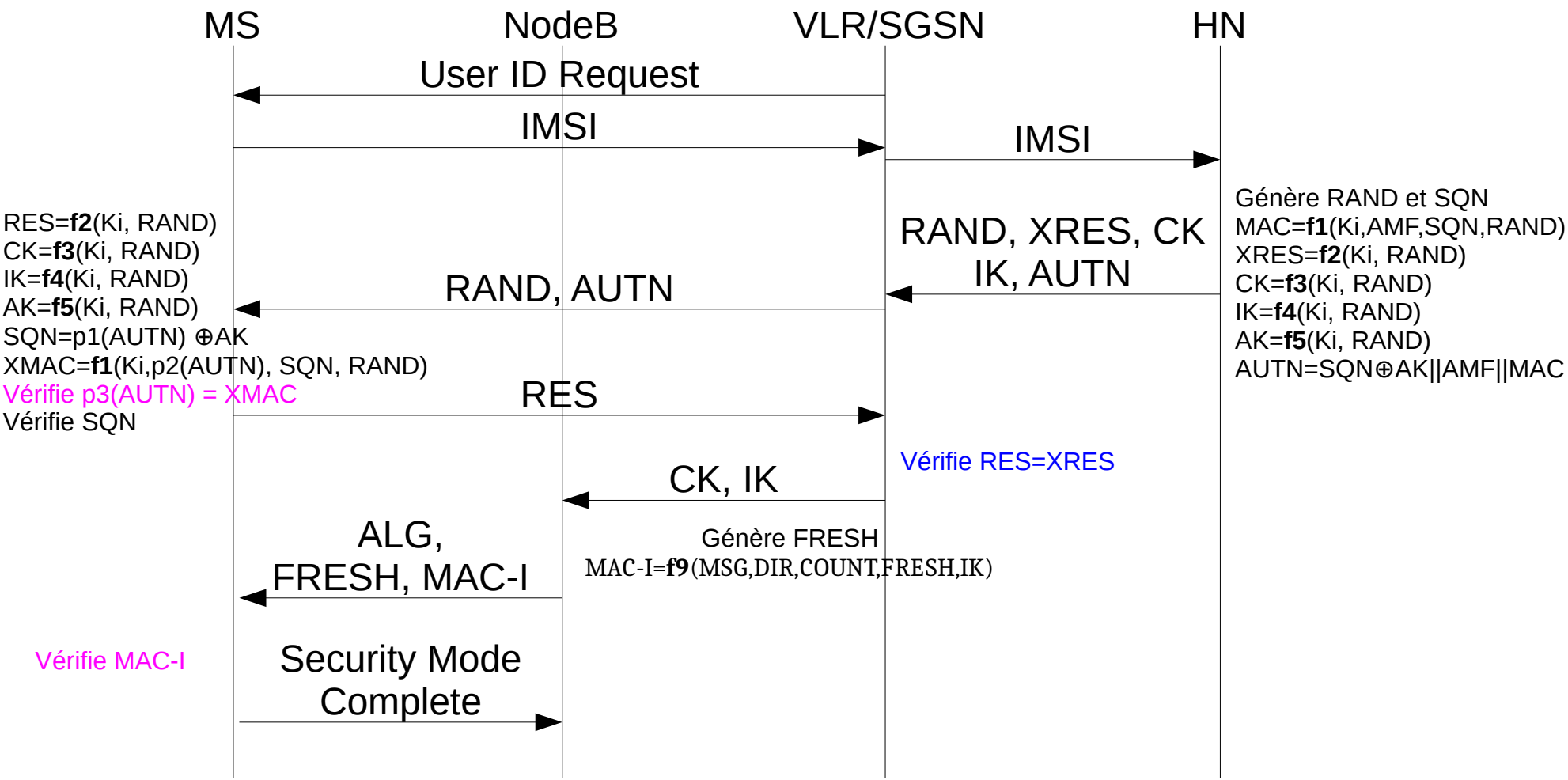
- Authentication and Key Agreement (AKA)
- Authentification mutuelle
- RFC 3310 / RFC 4187 (EAP-AKA)
- 3G : 10 algorithmes (de f0 à f9)
- 4G : **KDF** (Key Derivation Function)
- Chiffrement par XOR :
  - KeyStream=**f8**(CK,COUNT,BEARER,DIR,LEN)

Paramètres et sigles 3G

Parameter	Definition	Bit size
K	Pre-shared secret key	128
RAND	Random challenge	128
SQN	Sequence number	48
AK	Anonymity Key	48
AMF	Authentication Management Field	16
MAC	Message Authentication Code	64
CK	Cipher Key	128
IK	Integrity Key	128
RES	Response	32-128
X-RES	Expected Response	32-128
AUTN	Authentication Token	128 (16+64+48)
AUTS	Authentication re-Synchronisation Token	96-128
MAC-I	Message authentication code for data integrity	32

Page 33 de la référence [3]

Authentification 3G



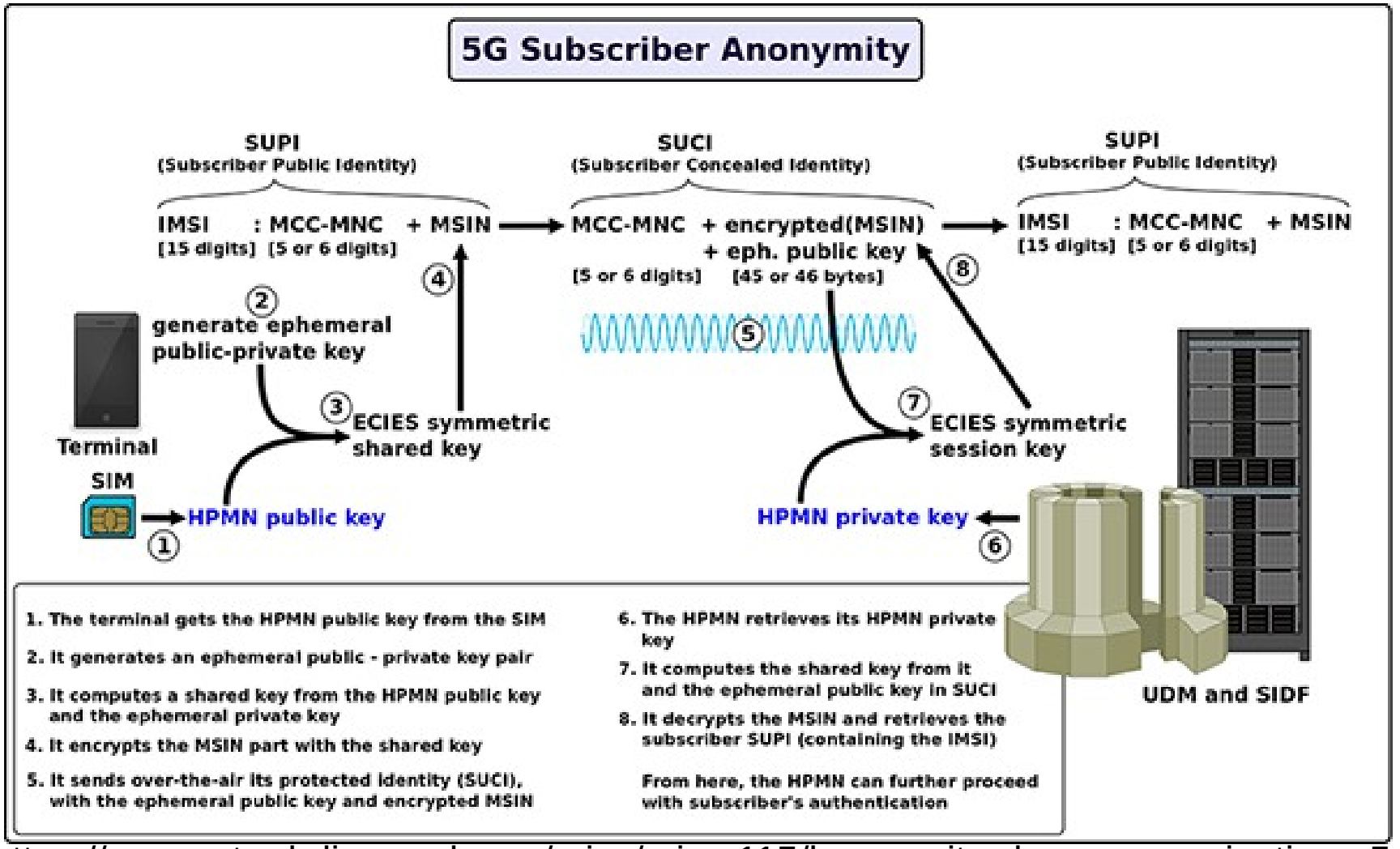
Authentification 4G

- Protection différenciée pour les liens AS et NAS
  - **AS** : Access Stratum UE<=>eNB
  - **NAS** : Non Access Stratum UE<=>MME (Mobile Management Entity)
- Ajout de K_{ASME}=**KDF**(CK,IK,SNid,SQN⊕AK)
  - SN identifier (Serving Network)
- Ajout de K_{eNB}=**KDF**(K_{ASME})

Authentification 5G

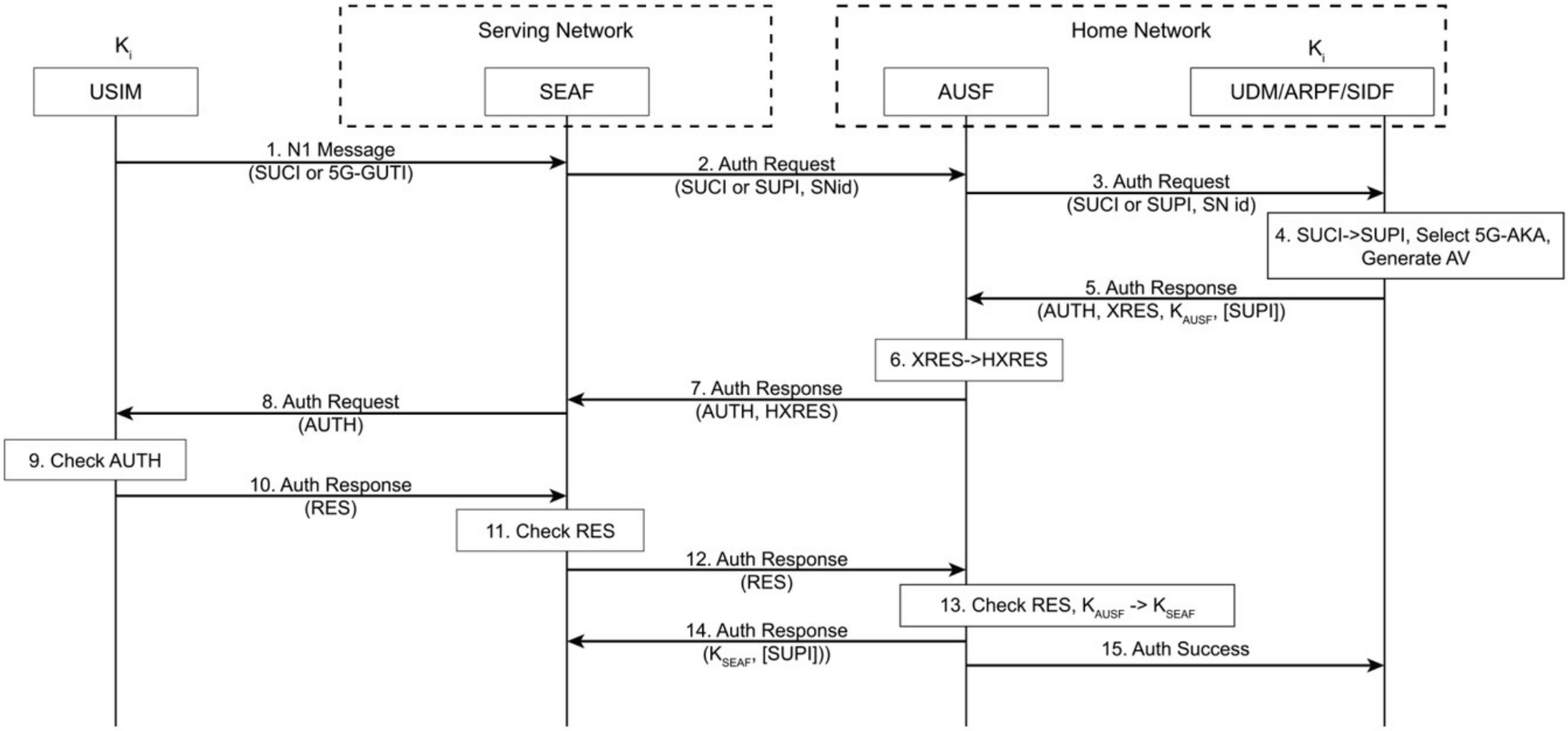
- Norme 3GPP TS 33.501
- **ECIES** (Elliptic-Curve Integrated Encryption Scheme) – courbes X25519 et secp256r1
- Les terminaux 5G n’envoient plus leur IMSI en clair sur l’interface radio
- Clé publique **HPMN** sur la carte ISIM

Anonymisation 5G



https://connect.ed-diamond.com/misc/misc-115/la-securite-des-communications-5g

Authentification 5G



https://blogs.univ-poitiers.fr/f-launay/2021/06/28/la-securite-des-reseaux-mobiles-part-5/

Références

- http://www.3gpp.org/
- http://fr.wikipedia.org/
- [3] Thèse « UMTS Authentication and Key Agreement » de Jon Robert Dohmen et Lars Sømo Olaussen 2001