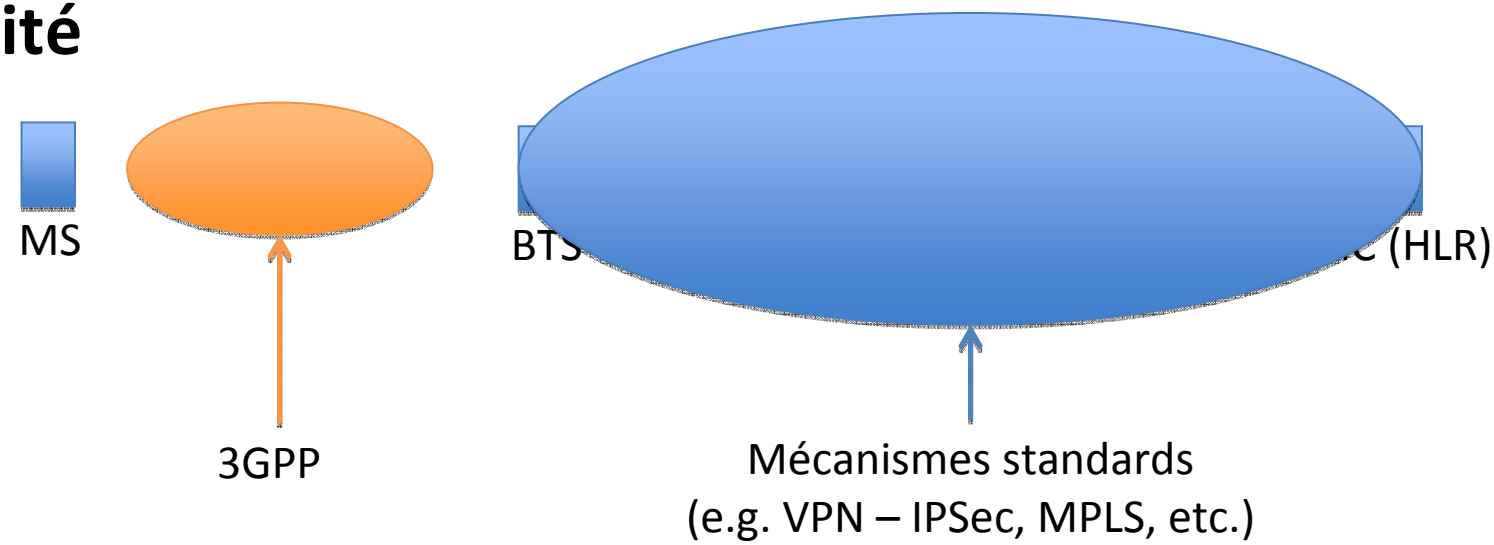
Fonctions de sécurité

Semaine 2

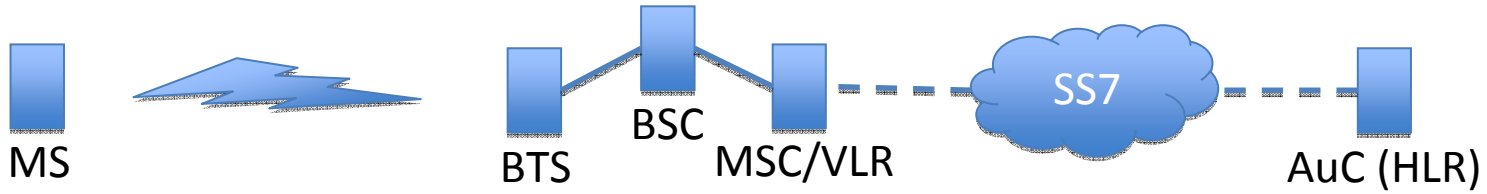
Sécurité



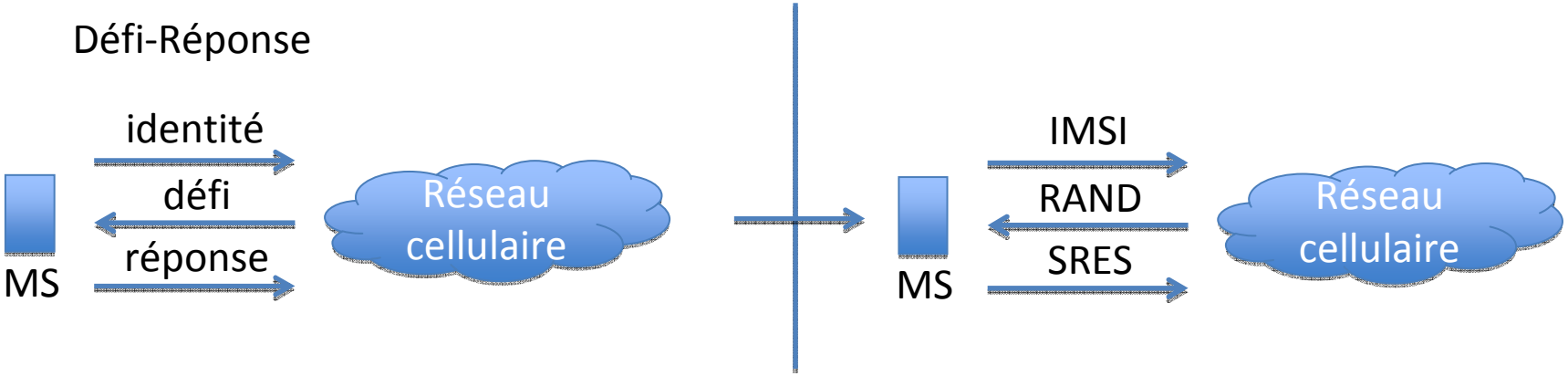
Fonctions de sécurité :

- Authentification du terminal par le réseau
  - Eviter un accès frauduleux au réseau
- Chiffrement des données et de la signalisation
  - Garantir la confidentialité des données transmises
- Allocation dynamique d'une identité temporaire transmise en mode chiffré
  - Garantir confidentialité de l'identité de l'utilisateur

Authentification du mobile

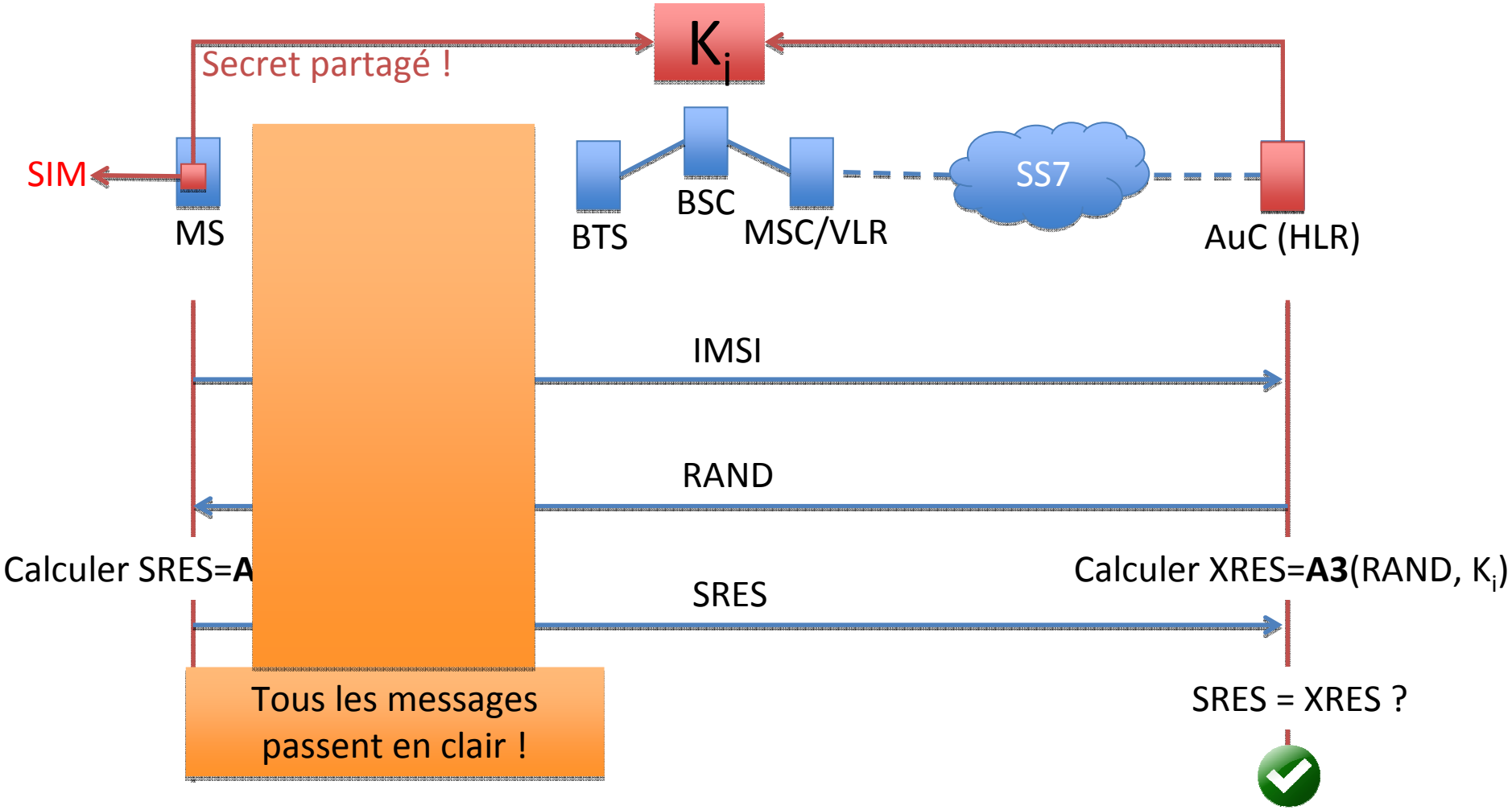


AuC = Authentication Center (Centre d'authentification)



RAND=RANDom (Valeur aléatoire)

SRES=Signed RESponse (Réponse signé)



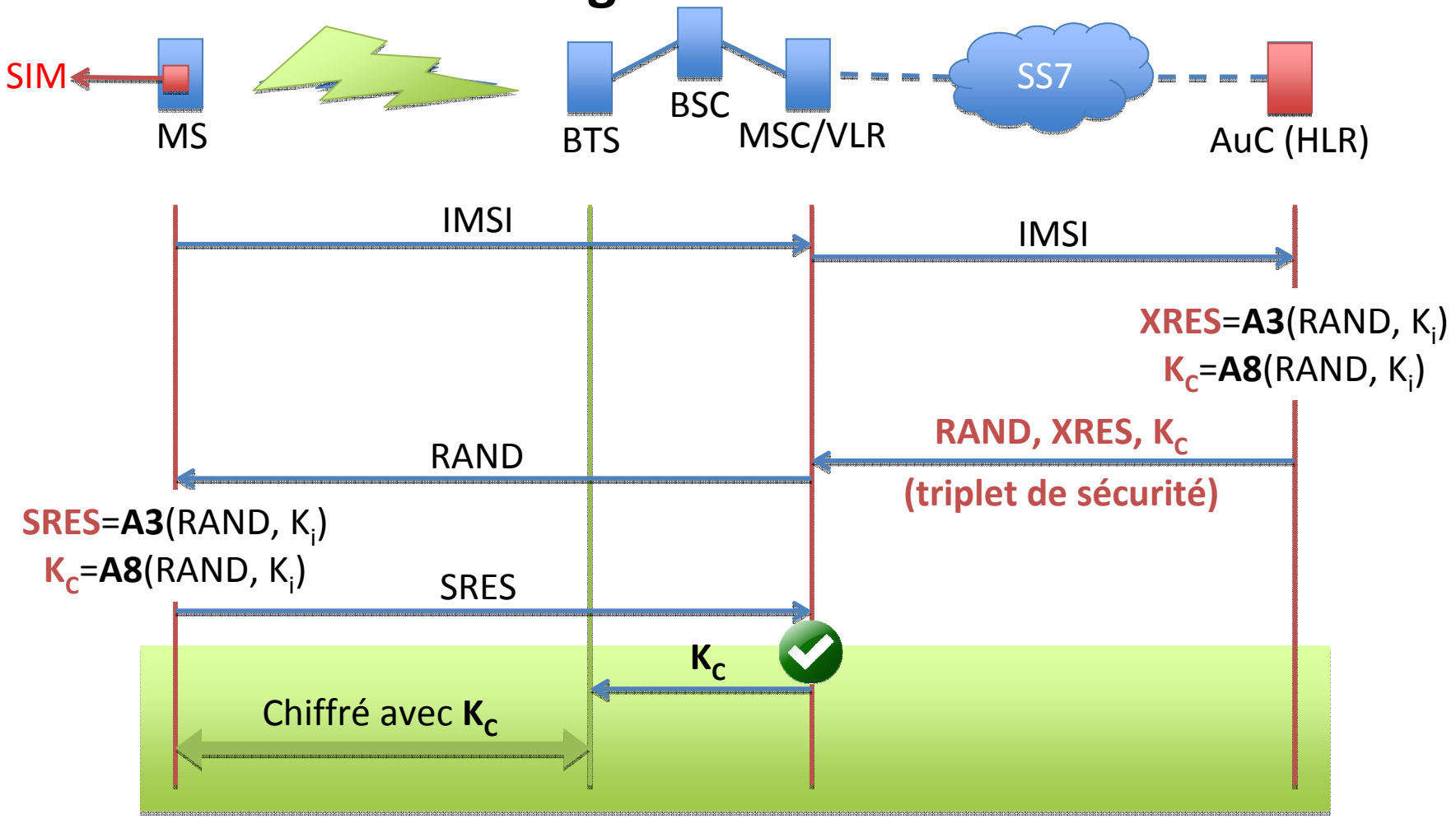
A3 – algorithme à sens unique (difficilement réversible)

K_i = 128 bits, RAND = 128 bits, SRES = 32 bits

Pour trouver K_i il faut plusieurs milliers de pairs RAND, SRES

Avec un couple (RAND, SRES) n'importe quel équipement du réseau peut identifier un abonné

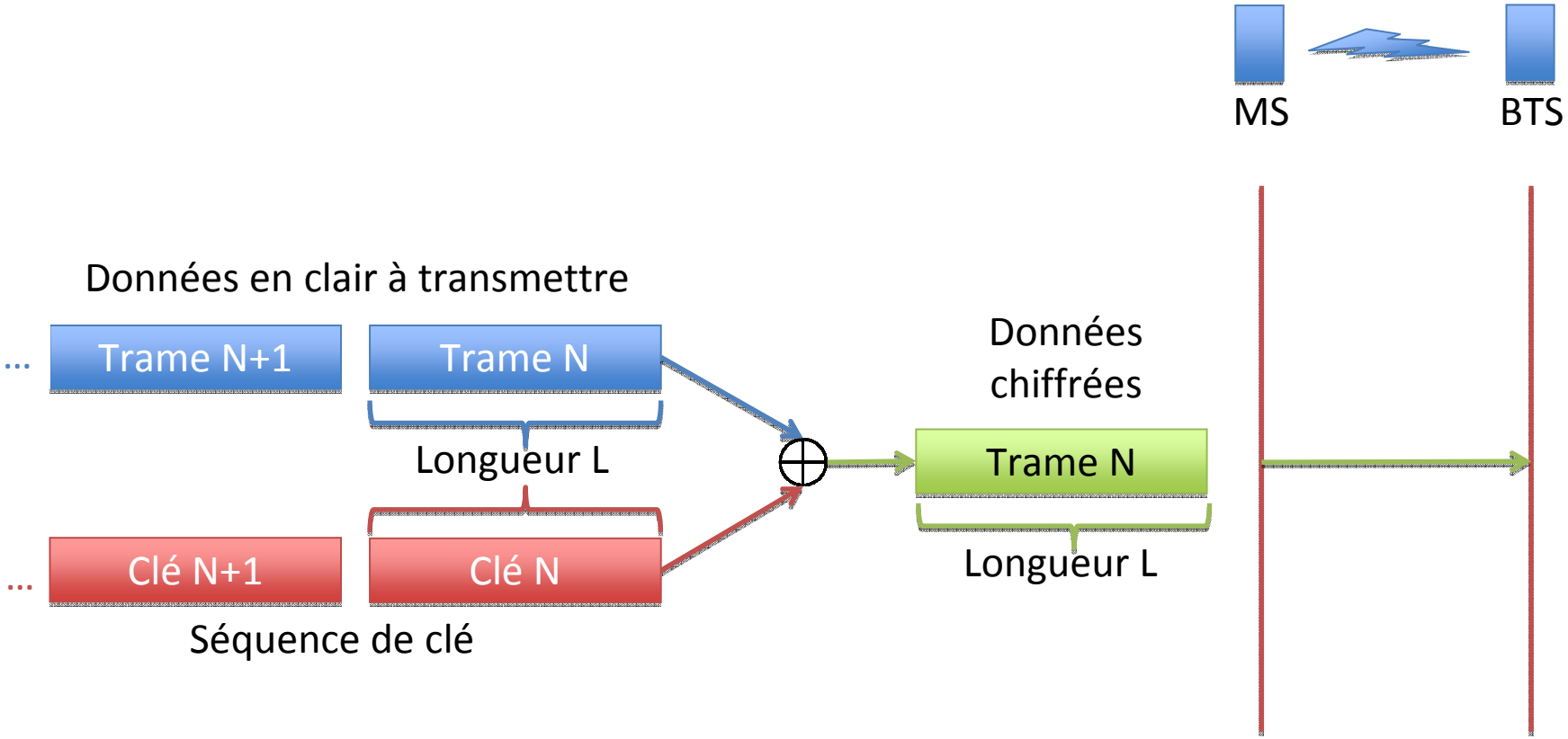
Chiffrement des échanges – clé de session



Il faut chiffrer chaque trame !

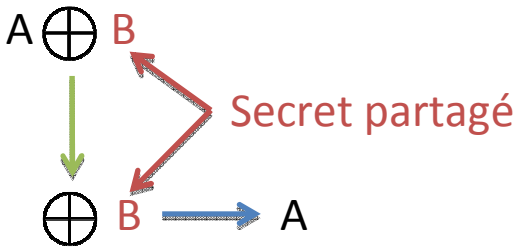
- Impossible d'interroger l'AuC pour chaque trame (chiffrement+déchiffrement)
- Le secret partagé ne doit jamais quitter l'AuC (et la carte SIM)
  - Solution – génération d'une clef de session $\mathbf{K_c}$ pour le chiffrement (64 bits)

Chiffrement des échanges – principe

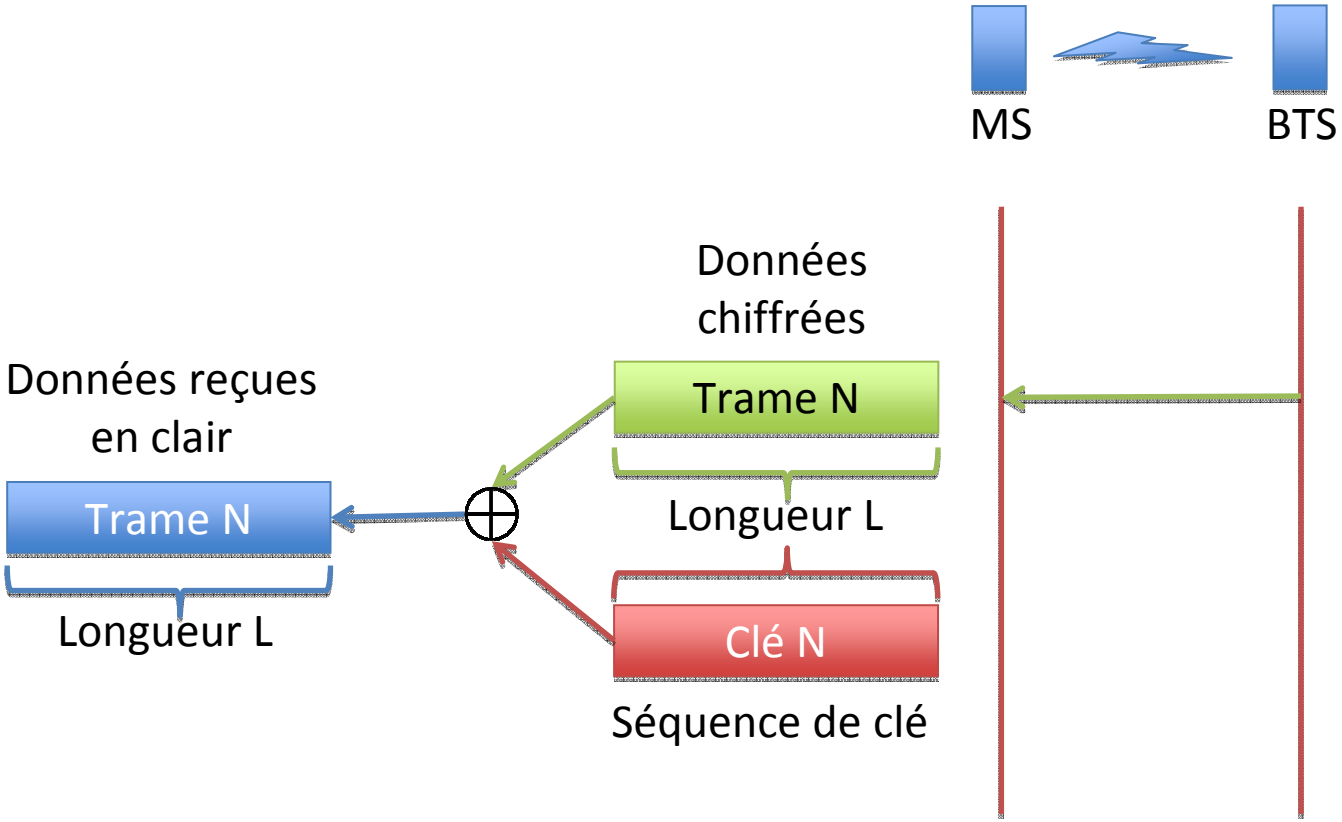


⊕ = OU exclusif

⊕	0	1
0	0	1
1	1	0

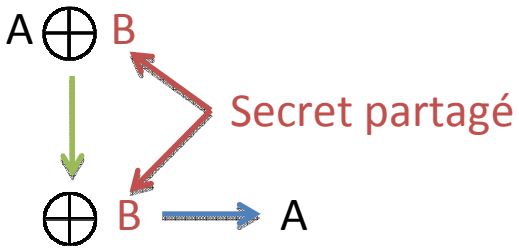


Chiffrement des échanges – principe

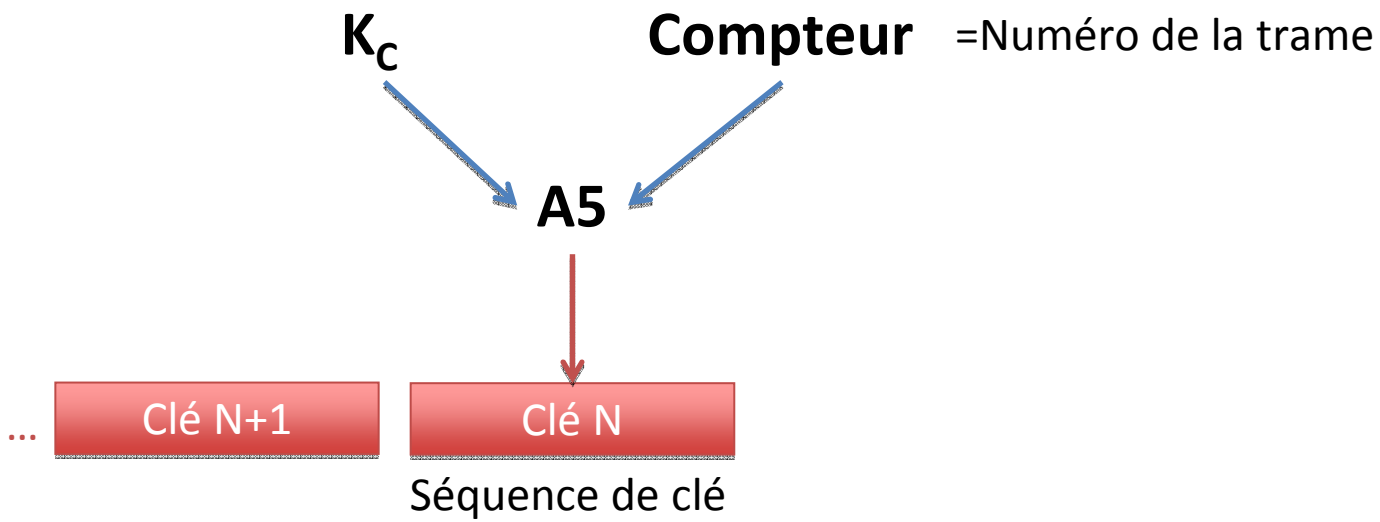


⊕ = OU exclusif

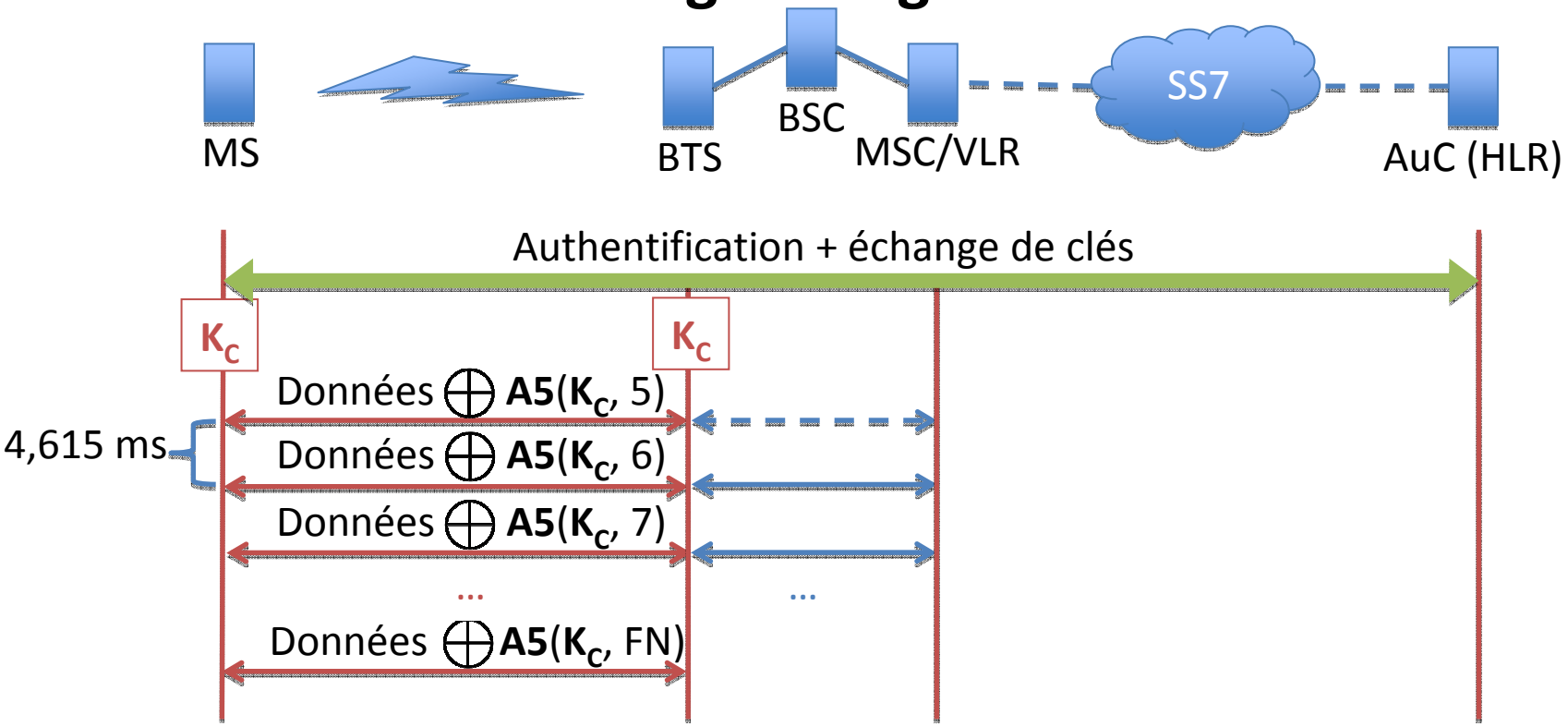
⊕	0	1
0	0	1
1	1	0



Chiffrement des échanges – principe



Chiffrement des échanges – algorithme



Clé $\mathbf{K_C}$ identique pendant toute la communication
•Clé renouvelée à chaque nouvelle communication

Séquence de chiffrement varie à chaque trame TDMA
•Compteur FN (Frame Number) : 0 à 2 715 647
•Incrémenté à chaque nouvelle trame
•Période : 2 715 647 * 4,1615 ms soit 3h 30 mn

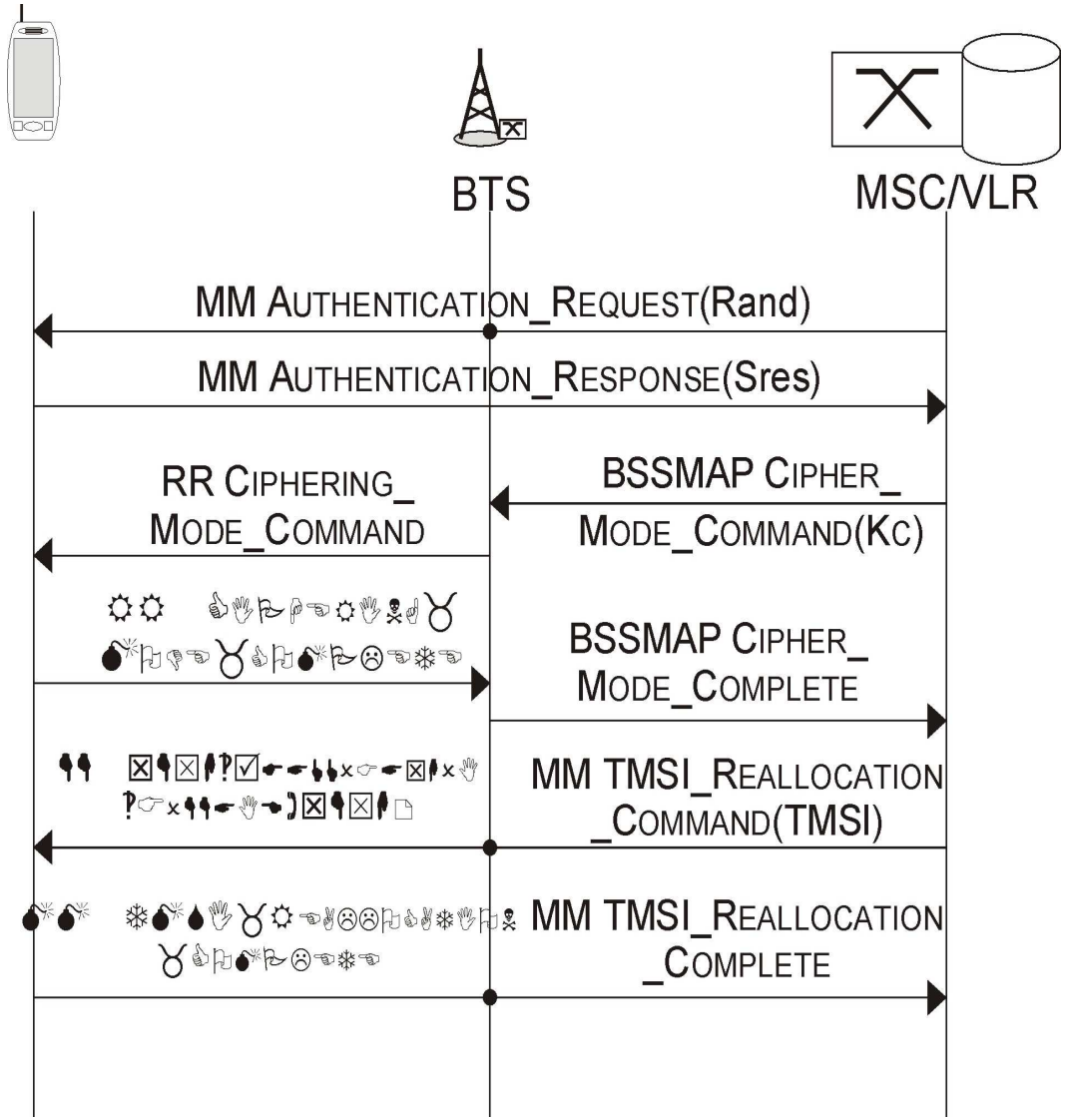
Algorithme **A5** dans le terminal et dans la BTS
•Même famille d'algorithmes dans tous les terminaux et les réseaux
•Algorithme **A5/1** : traditionnel
•Algorithme **A5/2** : moins protégé
•Algorithme **A5/3** : plus résistant

Identité temporaire - TMSI

(Temporary Mobile Subscriber Identity)

Sur 4 octets (contre 8 pour l'IMSI)
Portée locale (VLR)

Préserve la confidentialité de l'abonné
•Utilisé dans les messages de paging
•Pour les demandes d'authentification à la place de l'IMSI



Sécurité 3G/LTE

Fonctions de sécurité ajoutés pour la 3G/LTE
•Authentification du réseau par le terminal
•Vérification d'intégrité

	GSM	UMTS	LTE
Authentification du terminal	✓	✓	✓
Authentification du réseau	✗	✓	✓
Chiffrement de la signalisation, des données	✓	✓	✓
Vérification d'intégrité des messages de signalisation	✗	✓	✓
Confidentialité de l'identité	✓*	✓*	✓*

* sauf cas particulier