INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

Sécurité des Réseaux Cellulaires

Walid Bechkit, INSA-Lyon, INRIA-Agora

citi lab

Inria INVENTEURS DU MONDE NUMÉRIQUE

membre de UNIVERSITÉ DE LYON

Aperçu sur le contenu du cours

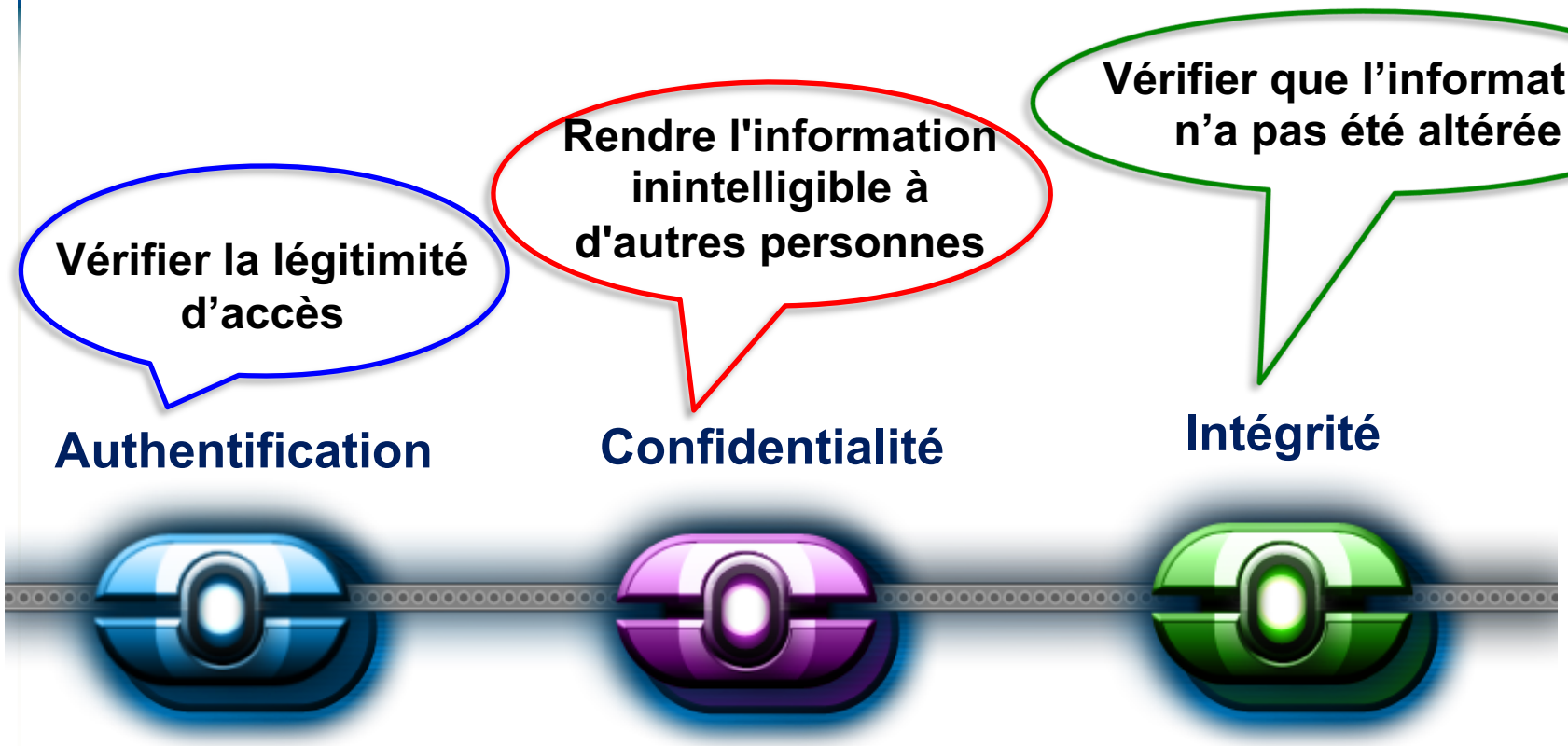
- Rappel de quelques notions de base
- Sécurité des réseaux de deuxième génération
- Sécurité des réseaux GPRS
- Sécurité des réseaux de troisième génération
- Sécurité des réseaux de quatrième génération

Principales références

- **Xavier Lagrange, Philippe Godlewski et Sami Tabbane, Réseaux GSM , Hermes, 5 éme edition, 2000, ISBN 2-7462-0153-4**
- **Xavier Sanchez, Hamadou Thioune, UMTS, Hermes,2 eme édition 2004. ISBN 1-905209-71-1**
- **Yannick Bouguen, Éric Hardouin, François-Xavier Wolff, LT, E et les reseaux 4G, EYROLLES, 2012, ISBN : 978-2-212-12990-8**
- **Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller and Valtteri Niem, LTE Security, John Wiley & Sons, 2011 , ISBN 978-1-118-35558-9**
- Bertrand Morel, Jean-Philippe Pastré, K Bedoui: Présentation de l'UMTS France Télécoms Orange
- Cours GSM/GPRS disponible sur : http://fr.slideshare.net/Garry54/gsm-4449773
- C. Demoulin, M. Van droogenbroeck. Principes de base du fonctionnement du réseau GSM. Revue de l'AIM, pages 3–18, N04, 2004
- …

Rappel de quelques notions de base

Rappel: services de sécurité



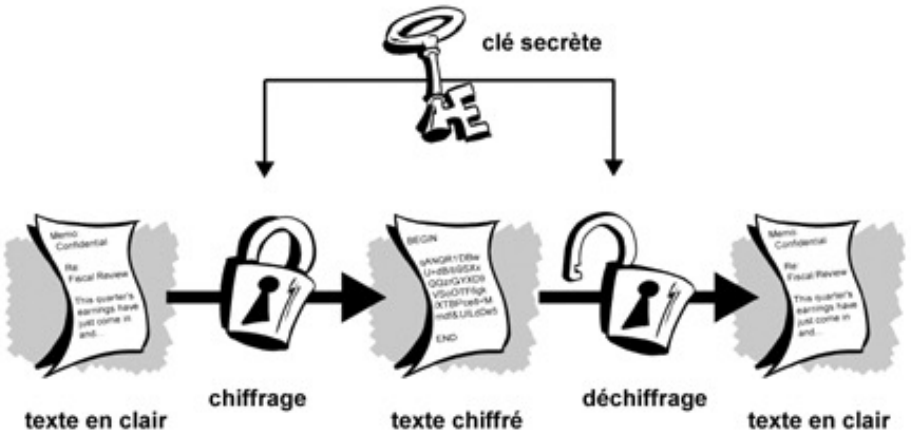
Rappel: chiffement symétrique Vs asymétrique

Chiffrement symétrique:

Même clé pour chiffrer et déchiffrer

\+ Rapide

\- Distributions des clés

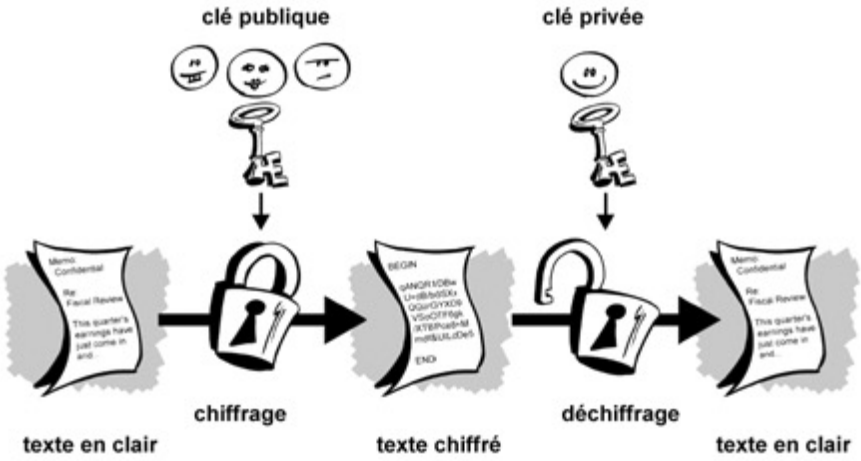


Chiffrement asymétrique:

Une clé publique pour chiffrer et une clé privée pour déchiffrer

\+ Pas de problème de distribution de clé

\- Lenteur (~ x1000)



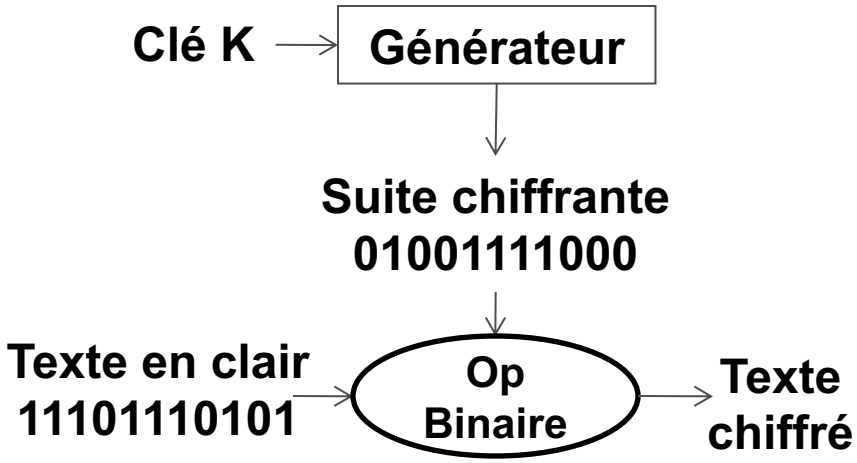
Rappel: chiffement symétrique

Chiffrement symétrique par flot

+ Rapide

- Vulnérable à à la cryptanalyse

Exemples: RC4, **A5/1**, etc.

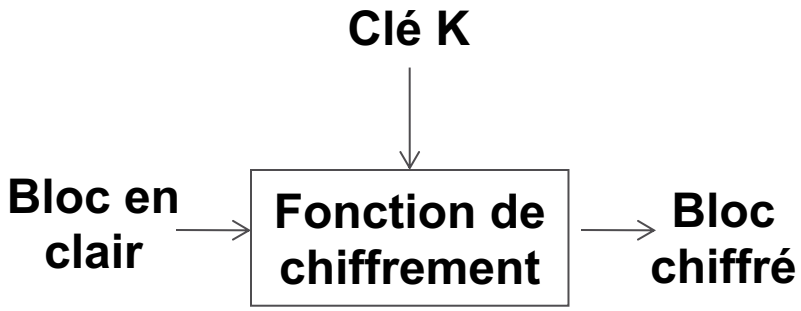


Chiffrement symétrique par bloc

+ Moins vulnérable à la cryptanalyse

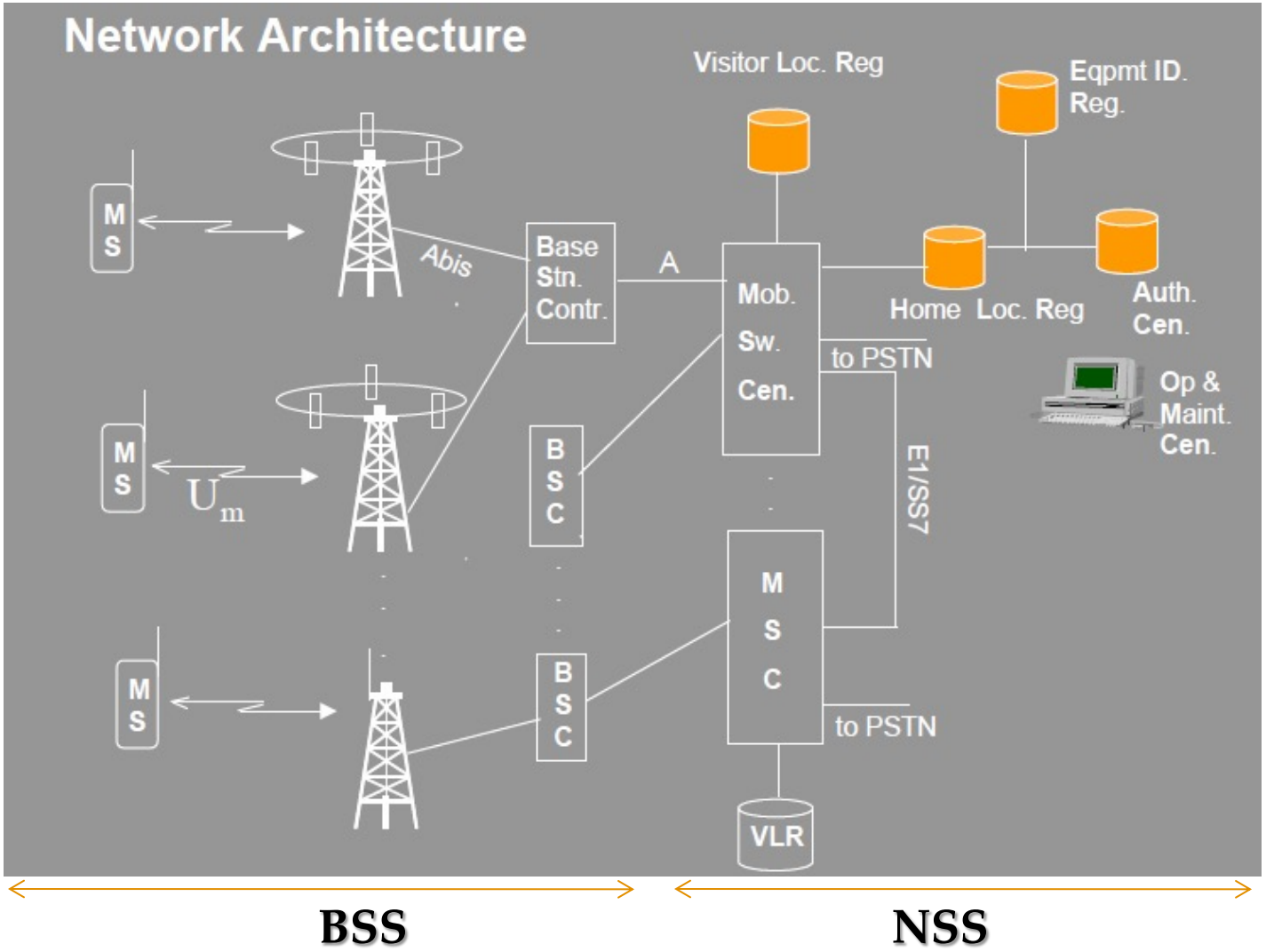
- Lenteur

- Exemples: DES, **AES,** etc.



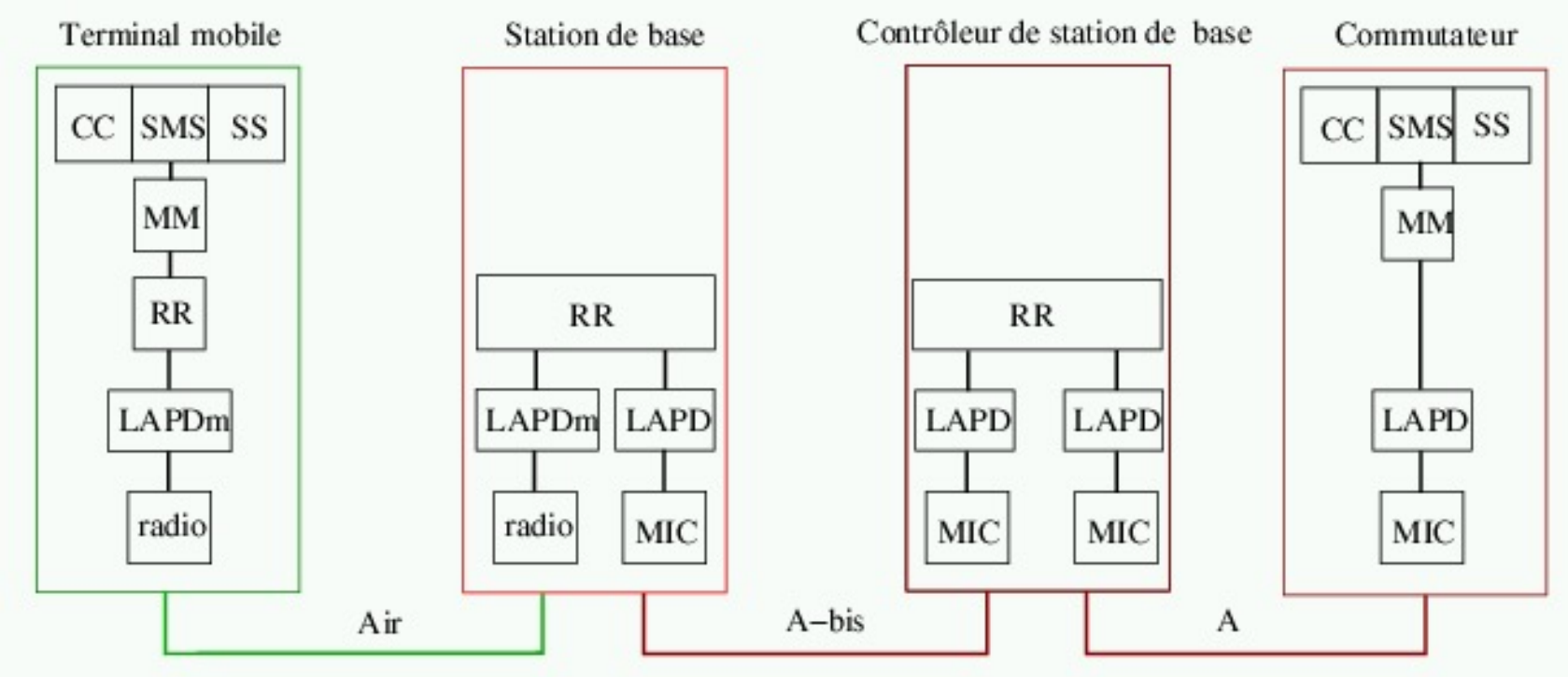
Réseaux GSM

Architecture physique



* Bhaskar Ramamurthi, GSM : Wireless Course , IIT Madras

Architecture protocolaire



* C. Demoulin, M. Van Droogenbroeck, Principes de base du fonctionnement du réseau GSM, Institut Montefiore, Belgique

Sécurité GSM

- **Vulnérabilité des communications radio → Besoin de**

  - Confidentialité de l'IMSI

  - Authentification

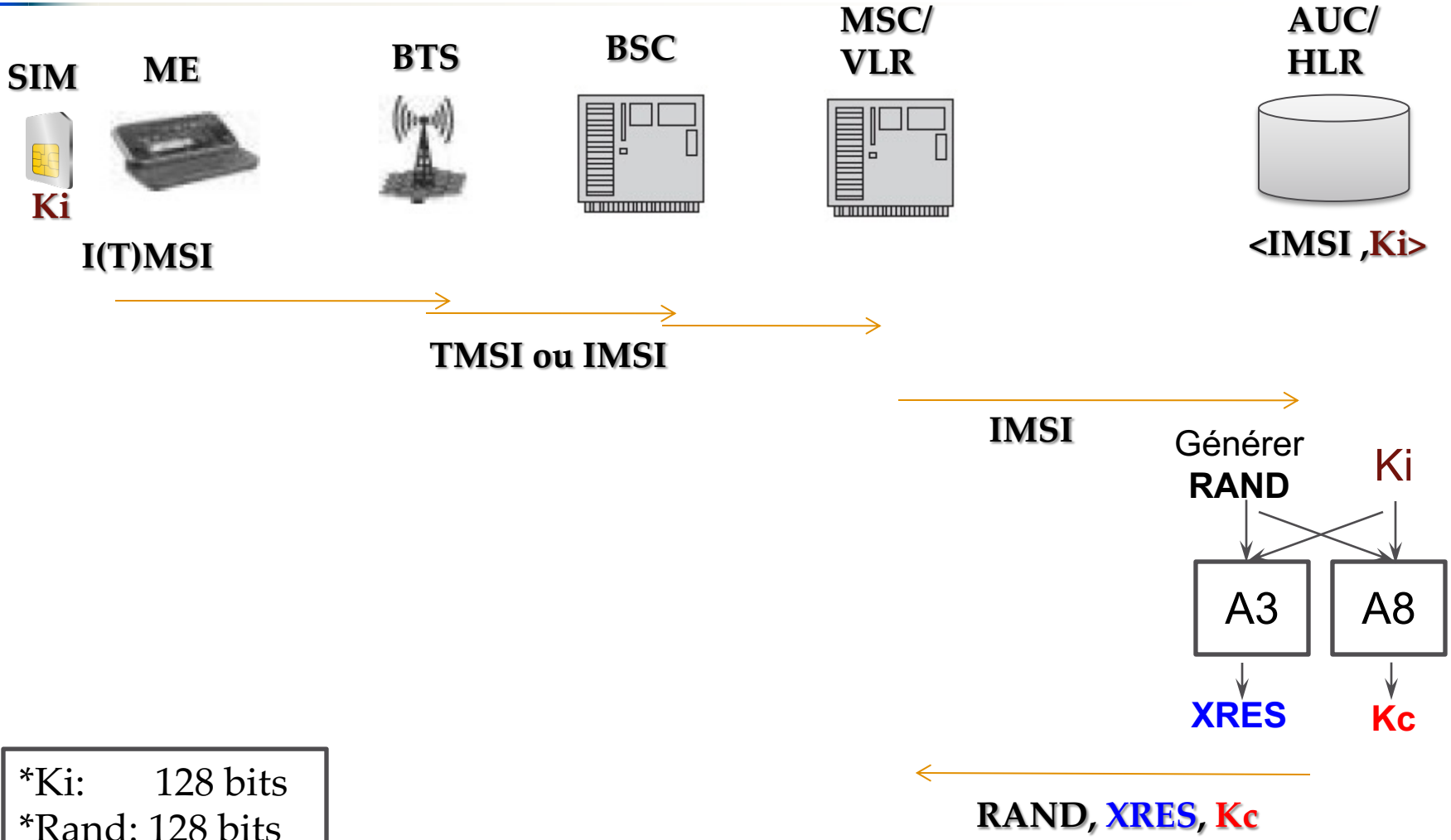
  - Confidentialité des données de trafic et de signalisation

  - Intégrité !

- **Les réseaux GSM assurent:**

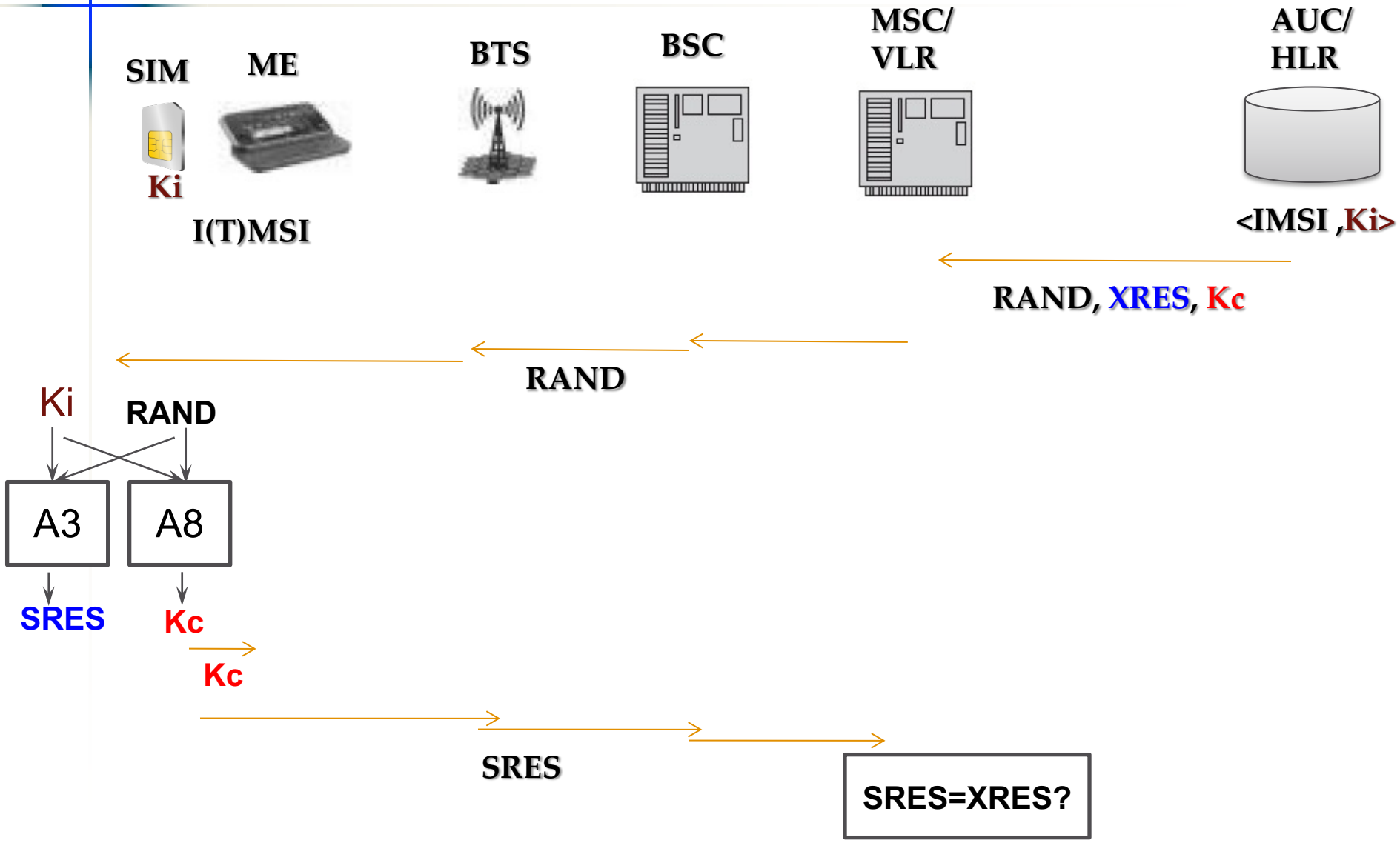
- La gestion des vols des équipements usagés
- Utilisation d'une identité temporaire TMSI attribuée par le VLR
- **Authentification** de chaque abonné auprès du réseau
- **Chiffrement** des communications entre le MS et la BTS

Authentification GSM

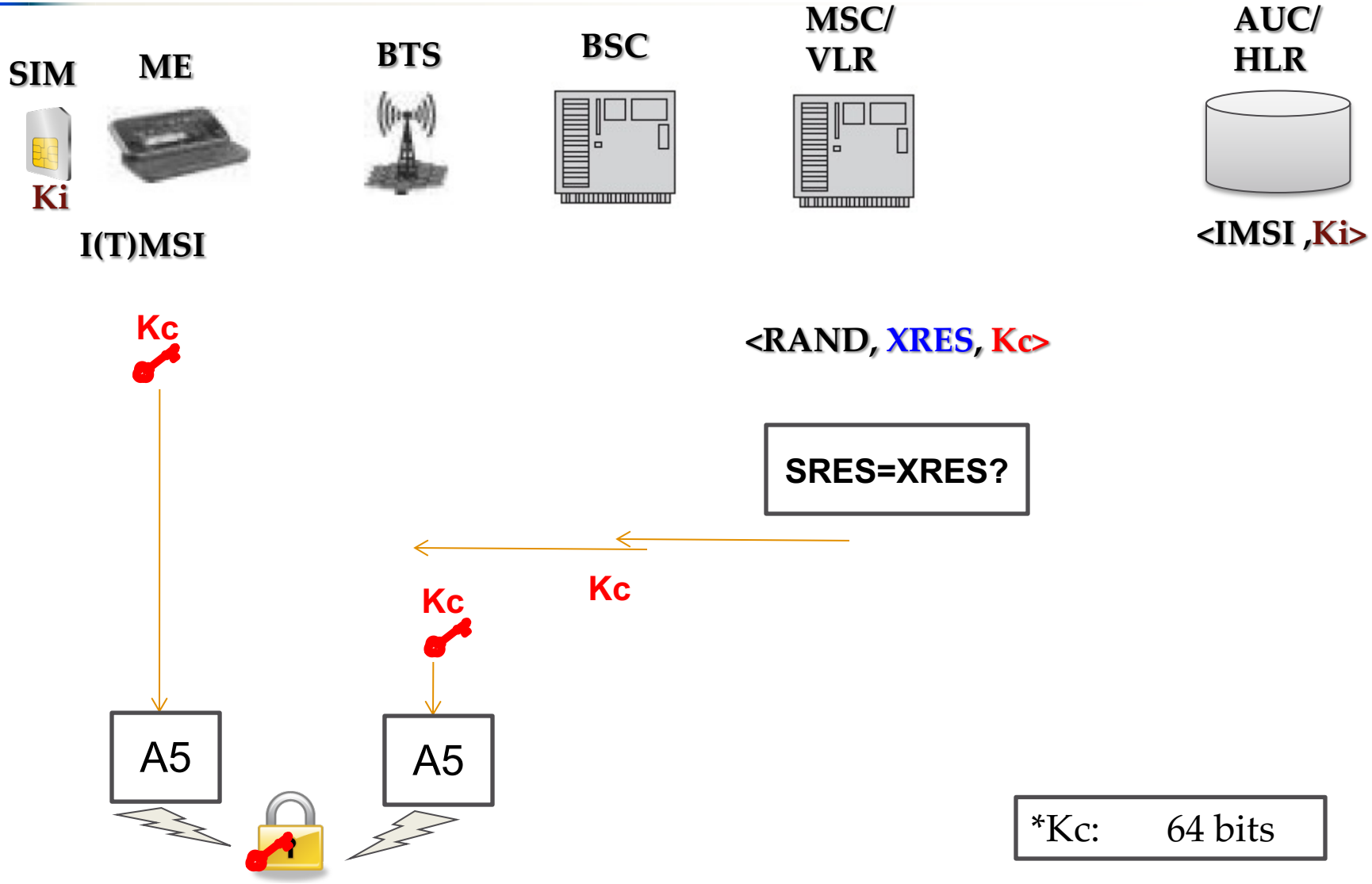


*Ki: 128 bits
*Rand: 128 bits
*XRES: 32 bits

Authentification GSM



Distribution de la clé de session



Authenfication des abonnés

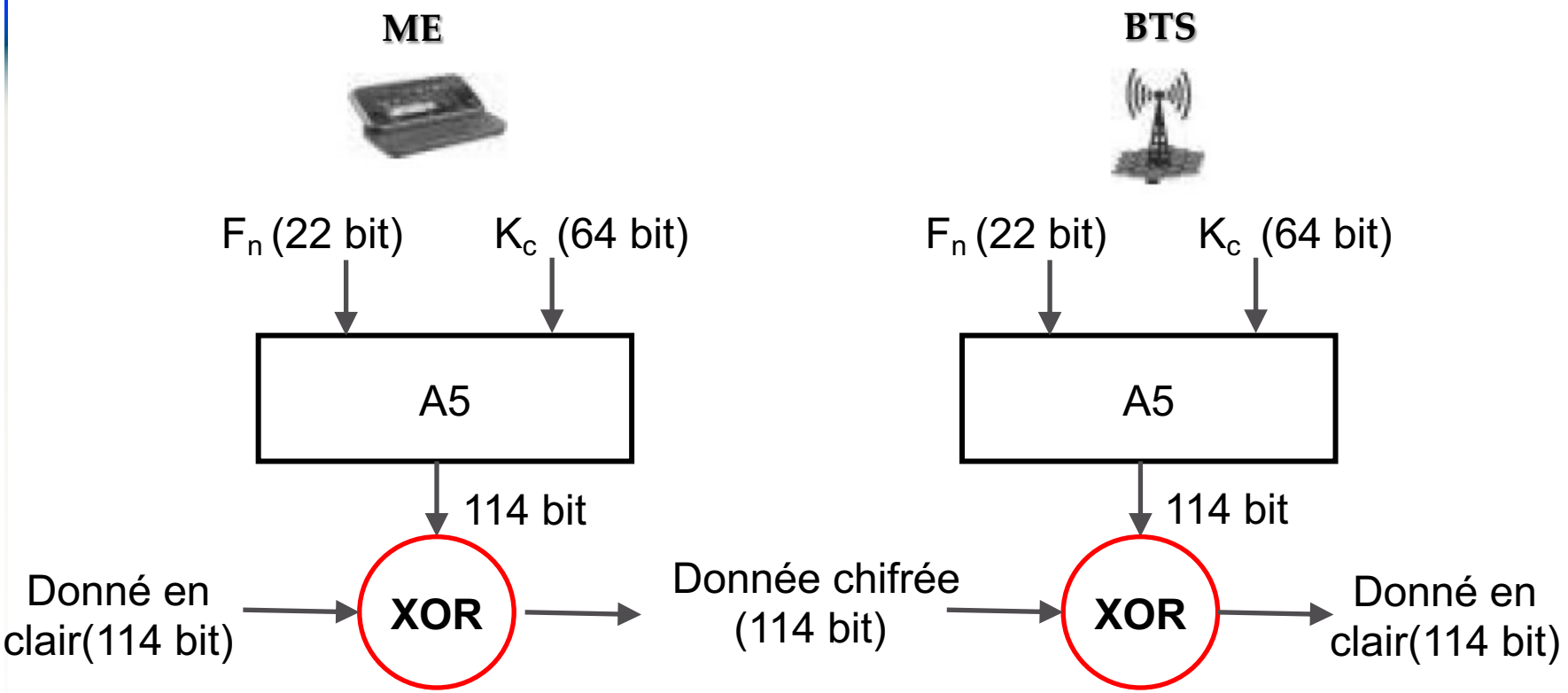
- L'authentification est déclenchée par le réseau:
  - L'abonné demande l'accès à un service (appel sortant, appel entrant, activation/ désactivation de services supplémentaires, etc.)
  - Premier accès après le démarrage du VLR/MSC
  - Mise à jour d'information de localisation , etc.

Algorithmes cryptographiques A3 et A8

- La carte SIM réalise le calcul A3 / A8 dans un espace sûr
- Même si la norme GSM ne recommande aucun algorithme, les opérateurs utilisent la procédure COMP128
- Les trois premières versions de COMP128 étaient initialement secrètes mais obtenues par «reverse engineering »

- Des chercheurs ont pu retrouver la clé grâce à environ 150 000 (challenge/response). Les algos COMP128 sont munis d'un compteur limitant le nombre de tentatives

Chiffrement de la voix en GSM (A5)



Fn: numéro de trame
Protocoles standardisés: A5/1, A5/2 (A5/0 no encryption)

Illustration du A5/1: https://www.youtube.com/watch?v=LgZAI3DdUA4

Sécurité : Quelques limites du GSM

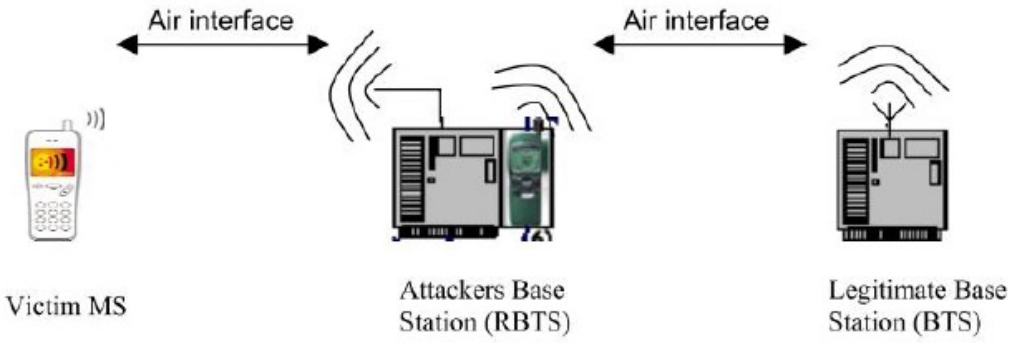
- **Authentification dans un seul sens (BTS malveillante !)**
- **Faiblesse des algorithmes A5/1 et principalement A5/2**
- **Les réseaux GSM n'assurent aucune intégrité des messages de contrôle ni de voix**
- **Les transmissions sont cryptées seulement entre MS et BTS**

- La clé de session est envoyée en clair entre le MSC/VLR et la BTS
- Vulnérabilité de COMP128v1
- Attaques par rejeu

Quelques attaques contre les réseaux GSM

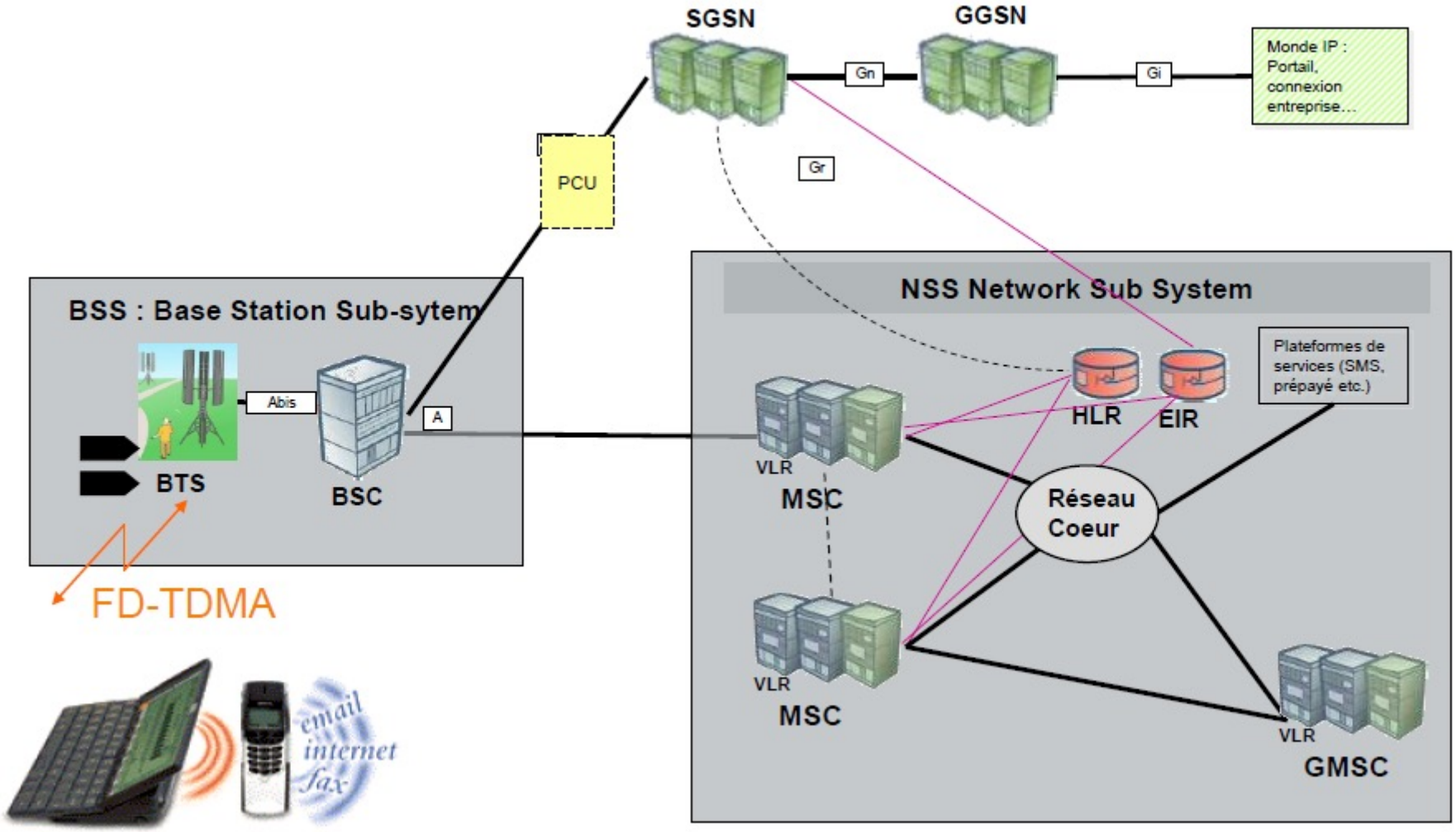
- **BTS Malveillante**

  (Rogue base stations)



- **Attaques contre l'authentification:**
  - Clonage physique des cartes SIM
  - Retrouver les K_i grâce aux challenges/responses
- **Attaques contre la confidentialité (retrouver Kc)**
  - Brute force 2^64 (réellement 2^54) (A5/1 → 2^40, A5/2 → 2^16)
  - Attaques par texte clair connu (peu pratique)

Evolution vers le GPRS (2.5 G)



* B Morel / JP Pastré, Réseau GPRS, France Télécom -Orange

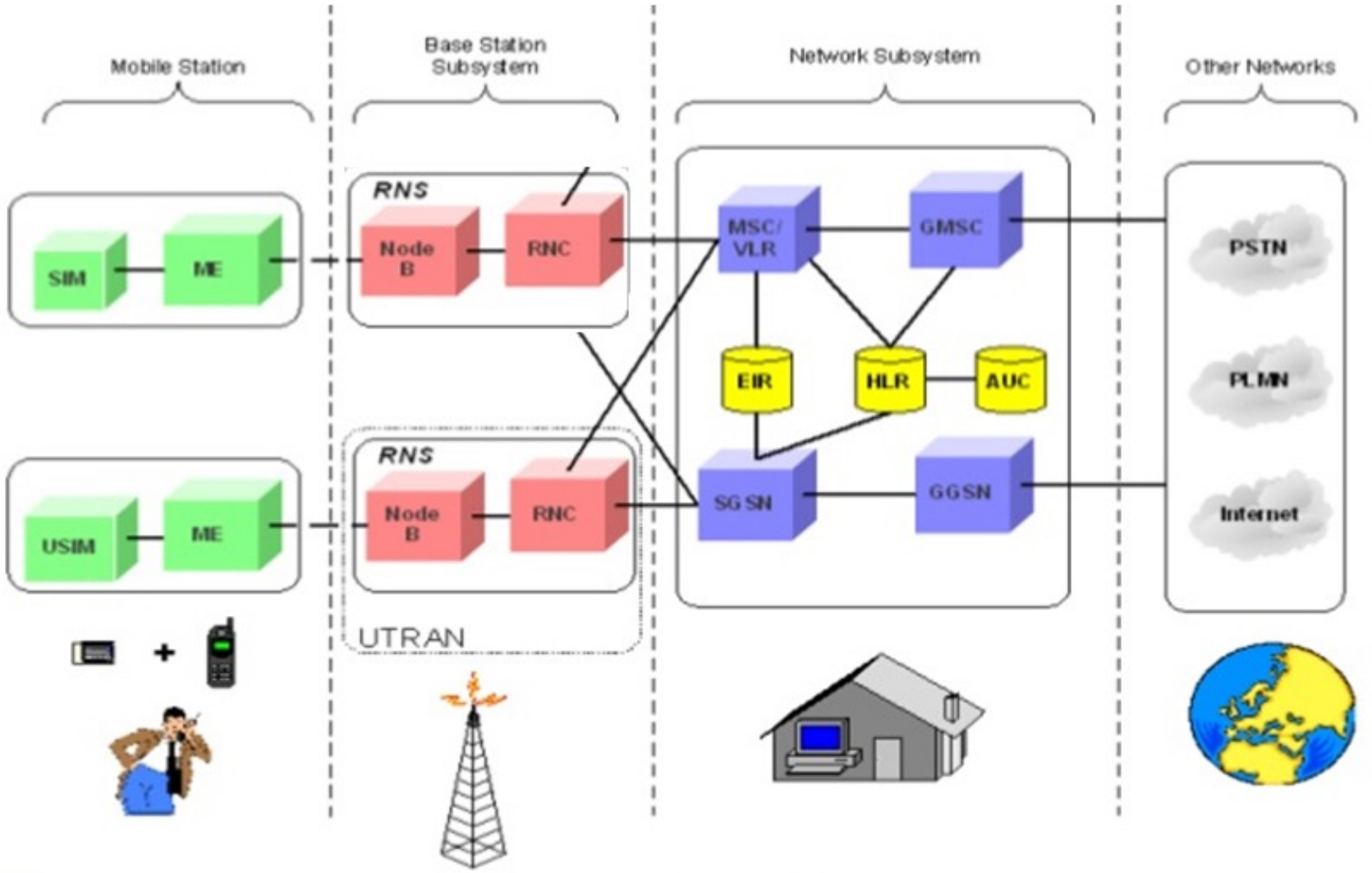
Sécurité dans les réseaux GPRS (2.5G)

- Attribution d'un identifiant temporaire P-TMSI par le SGSN
- Procédure d'authentification très similaire à celle du GSM (GPRS-Rand, GPRS-RES, GPRS-SRES)
- Génération similaire des clés de sessions GPRS-Kc

- Le chiffrement ne se fait plus au canal physique mais au niveau de la couche LLC (trame logique): avant segmentation des trames
- Le chiffrement se fait entre l'utilisateur et le SGSN
- Des algorithmes GEA (GPRS Encryption Algorithm) sont utilisés pour le chiffrement des paquets (très similaires aux algos A5)

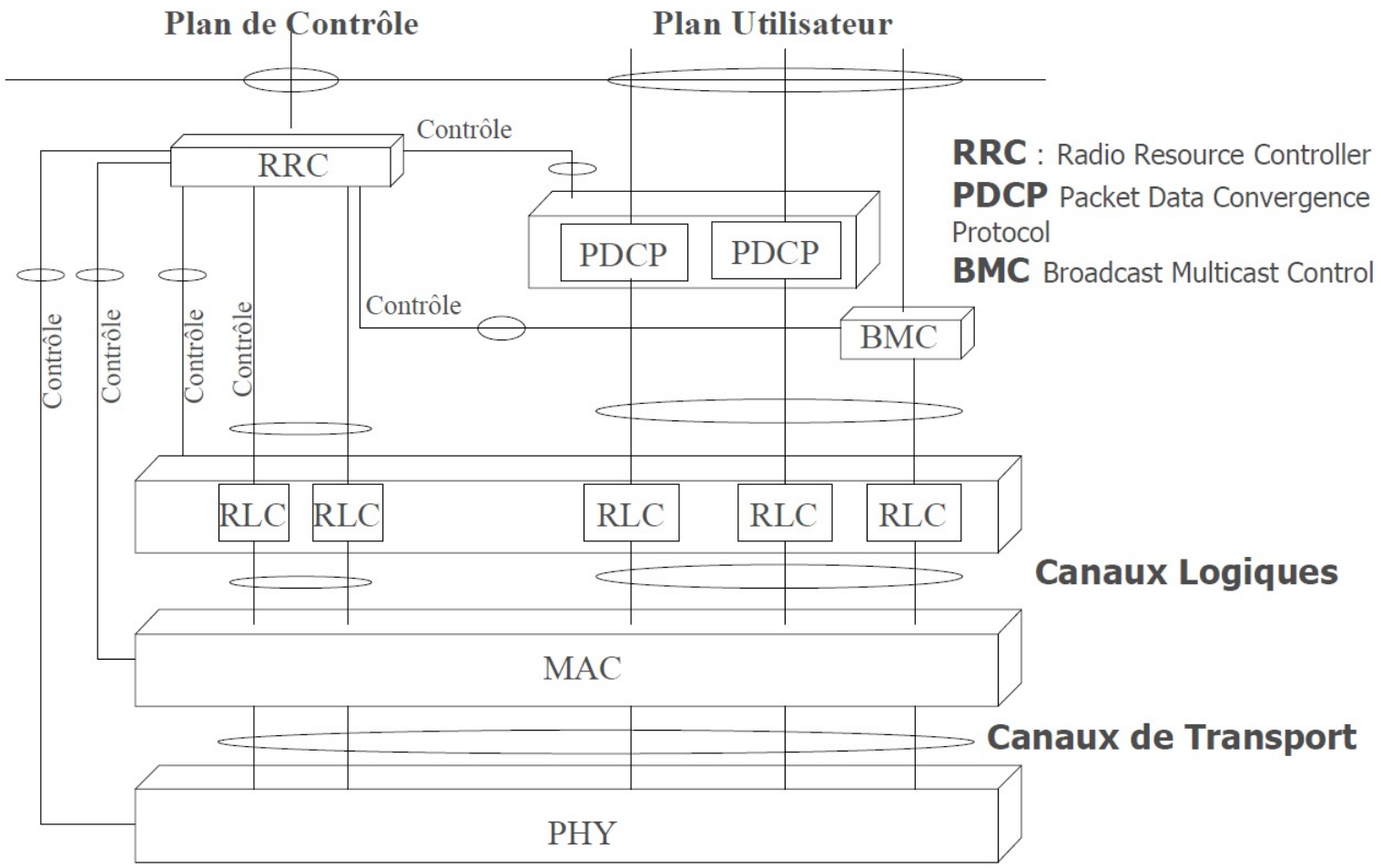
Réseaux UMTS

Architecture Physique



* L. ELAABIDI, cours UMTS, Cynapsys Software Enginnering

Architecture protocolaire



* A. BEYLOT, Architecture Protocolaire de l'UMTS cours UMTS, ENSEEIHT, Toulouse

Sécurité UMTS: principales nouveautés

- Authentification mutuelle
- Intégrité des échanges du plan contrôle
- Chiffrement entre UE et RNC (et non pas le nodeB)

- Nouveaux algorithmes pour la confidentialité et l'intégrité (UEA, UIA)
- Utilisation des clés de 128 bits (C_K et I_K)
- Utilisation des algorithmes publics

Sécurité UMTS

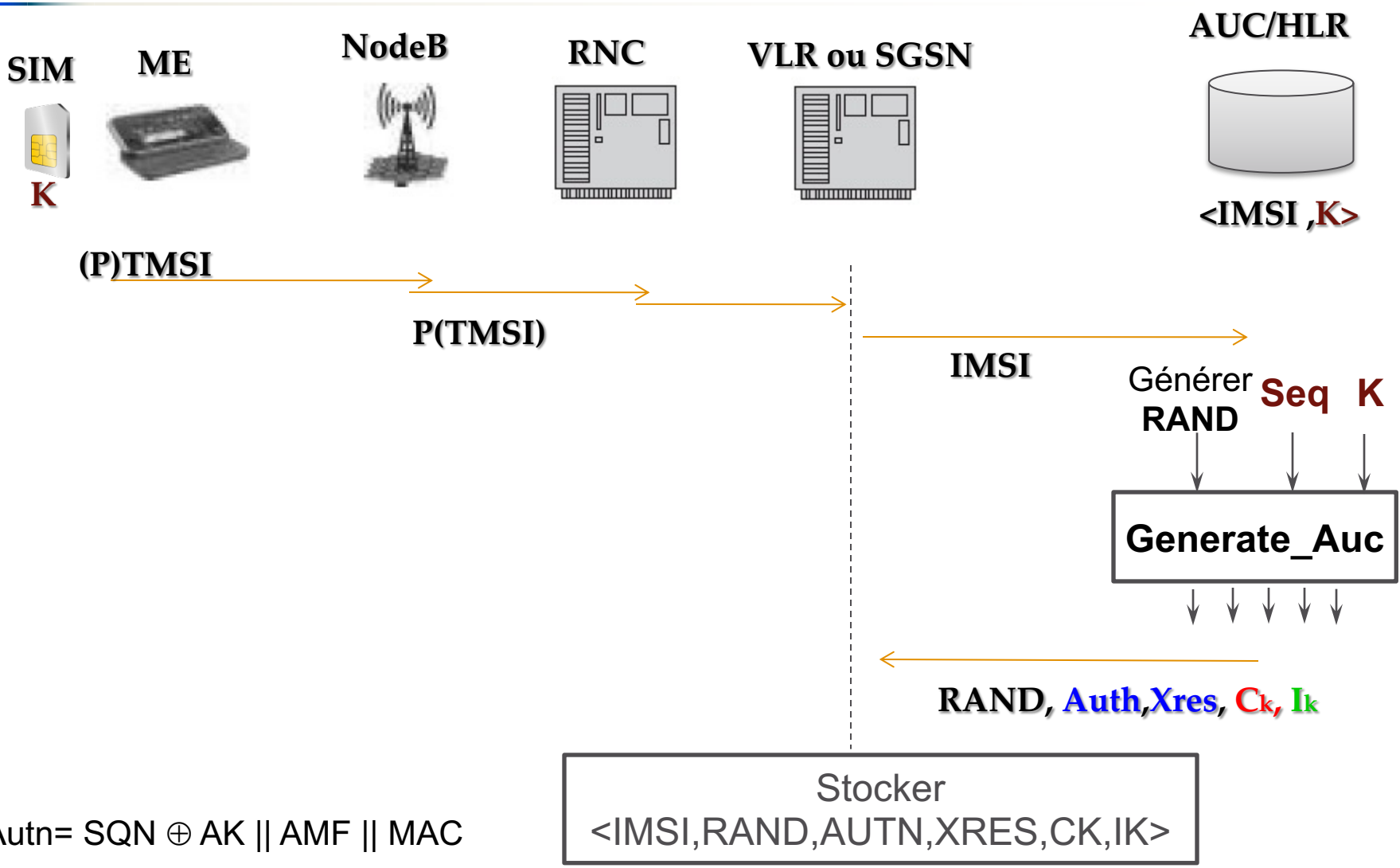
- L'authentification des utilisateurs à la carte USIM grâce à des codes PIN
- Identificateur temporaire :
  - TMSI : Domaine circuit (CS)
  - PTMSI : Domaine paquet (PS)
- Services de sécurité:
  - Authentification
  - Chiffrement
  - Intégrité des messages de contrôle

Sécurité UMTS

- K: clé secrète partagée entre l'AuC et USIM (128 bits)
- USIM et AuC ont un numéro de séquence synchronisé SQN
- RAND nombre aléatoire généré par l'AUC
- AMF: Authentification Management Field (Algo utilisés, durée de vie d'une clé, etc.)

- RES: Réponse au challenge RAND
- MAC: Code d'authentification à envoyer au mobile
- A_k : Clé utilisée pour masquer le numéro de séquence
- C_K : Clé de chiffrement (128 bits)
- I_K: Clé d'intégrité

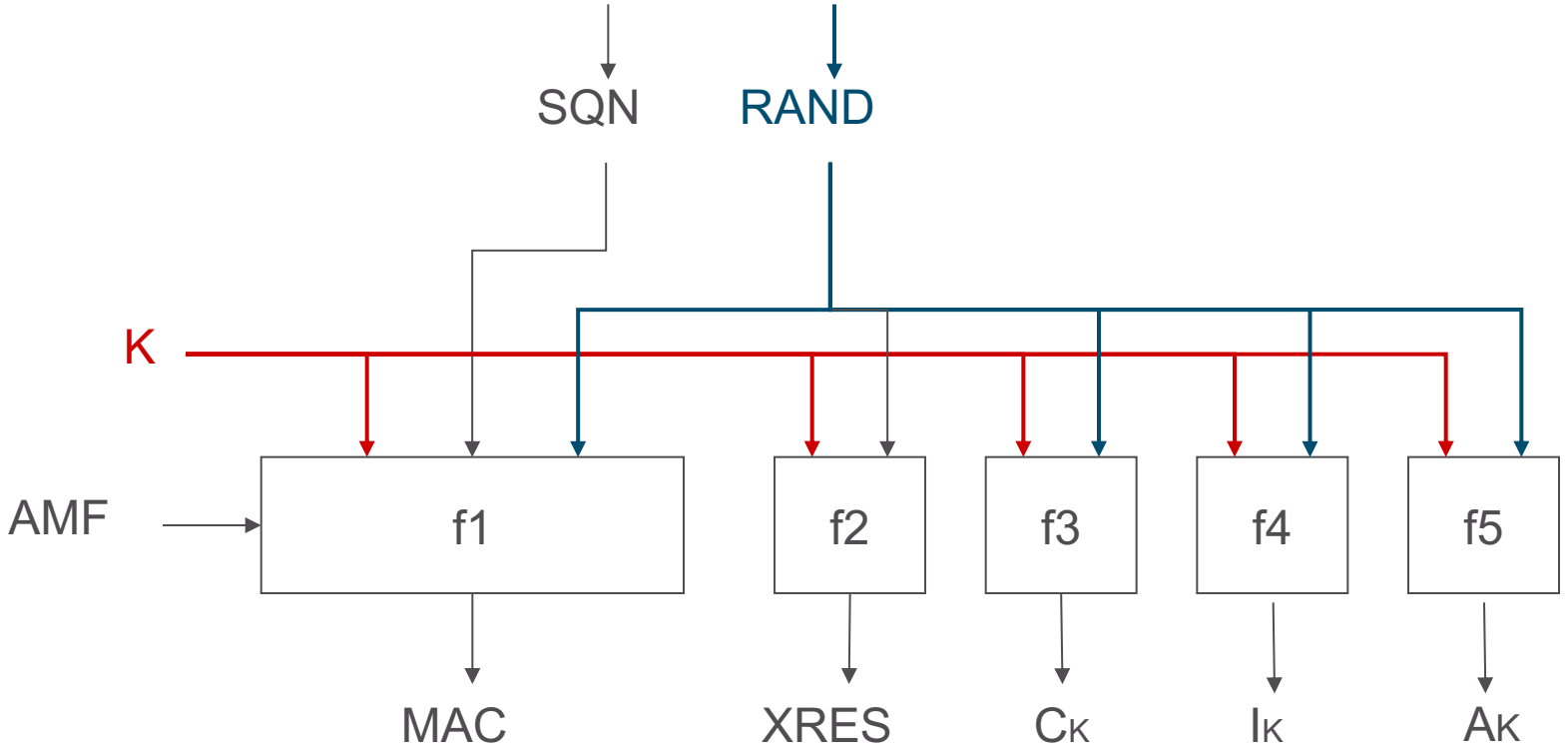
Authentification et génération de clés



*Autn= SQN ⊕ AK || AMF || MAC

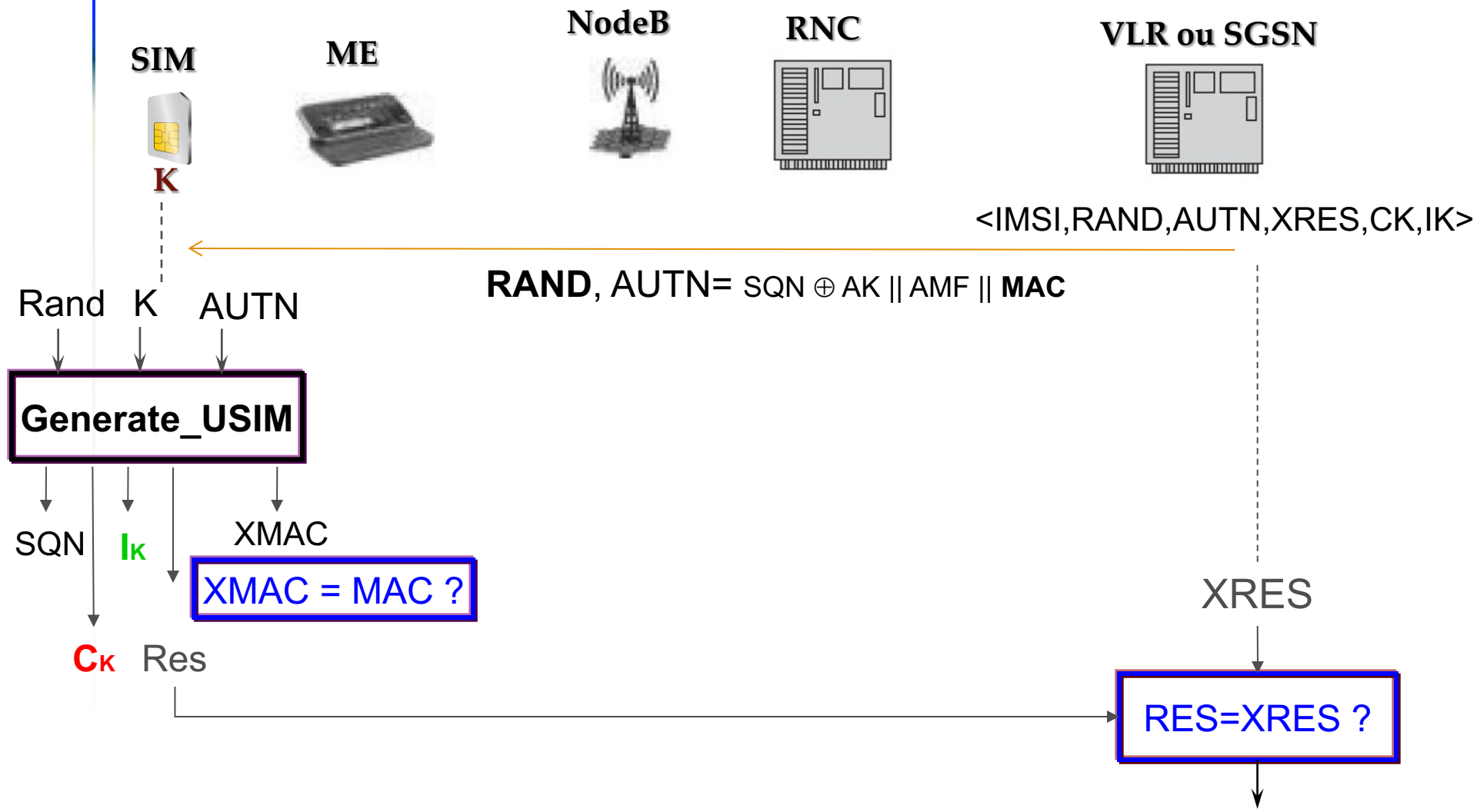
Authentification et génération de clés (Auc)

Détails de la fonction Generate_Auc:



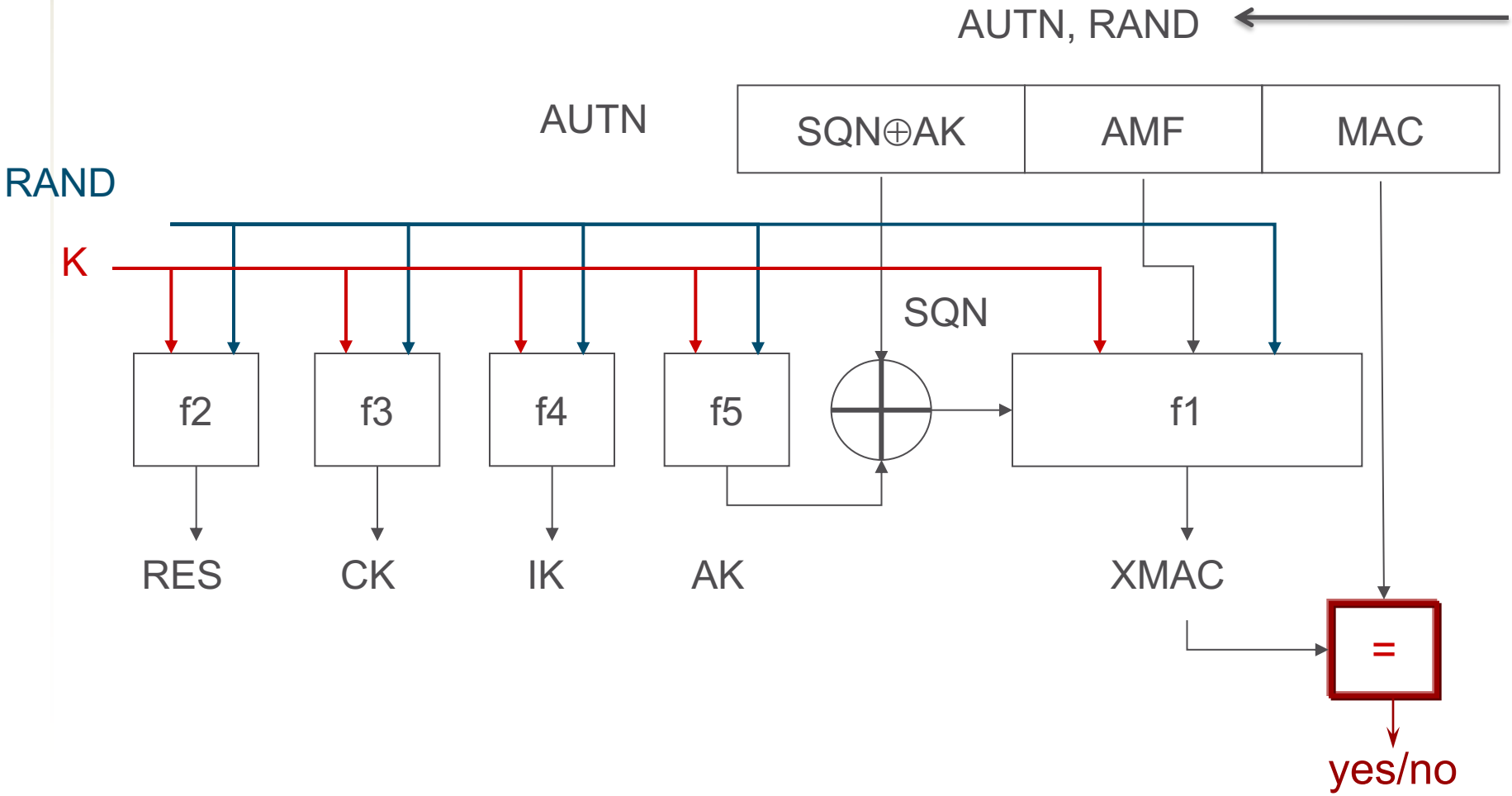
*Autn= SQN ⊕ AK || AMF || MAC

Authentification Mutuelle



Authentification et génération de clés: USIM

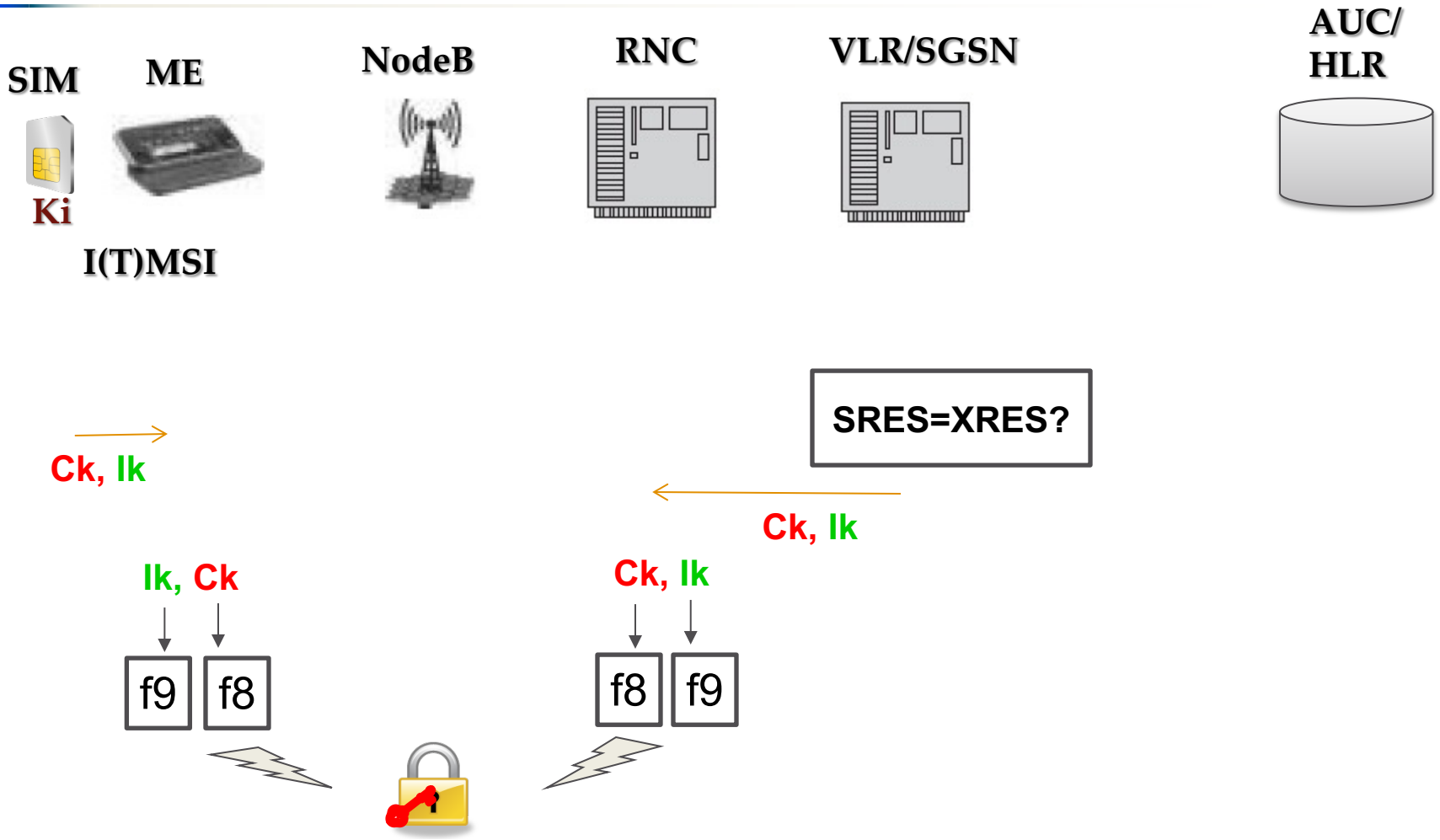
Détails de la fonction Generate_USIM:



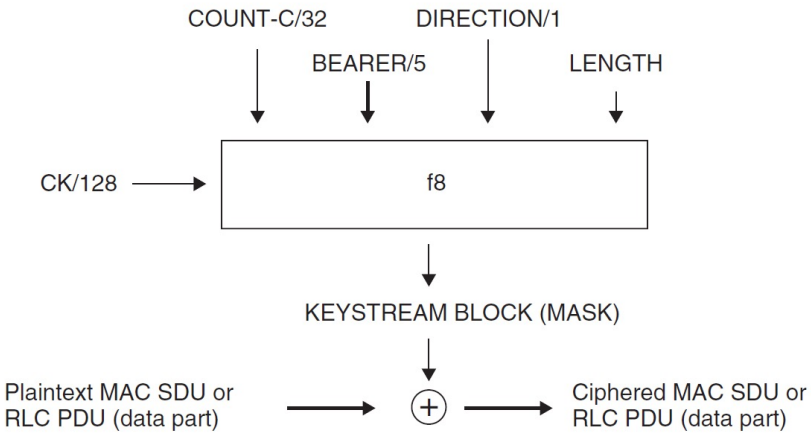
Algorithmes f1 … f5

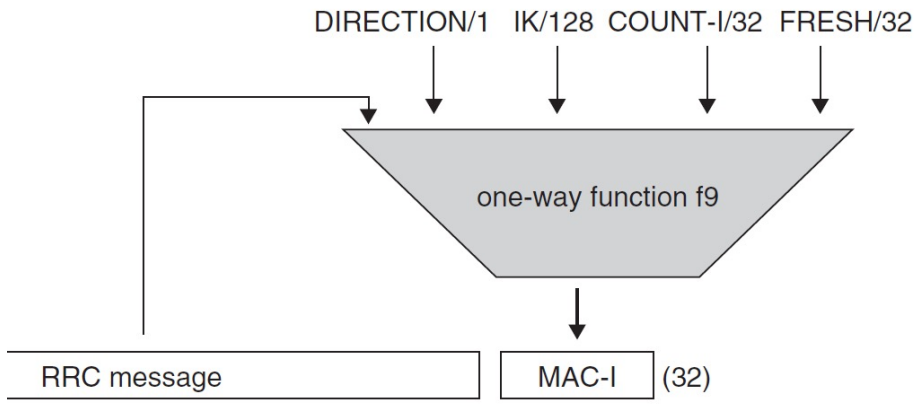
- Implémenté dans l'USIM et l'AuC
- Exécuté dans un espace sûr
- L'implémentation la plus utilisée: MILENAGE (connue aussi sous le nom de Comp128-4)
- Chiffrement par bloc (AES) avec des clés de taille 128 bits

Distribution de la clé de session



Confidentialité et intégrité





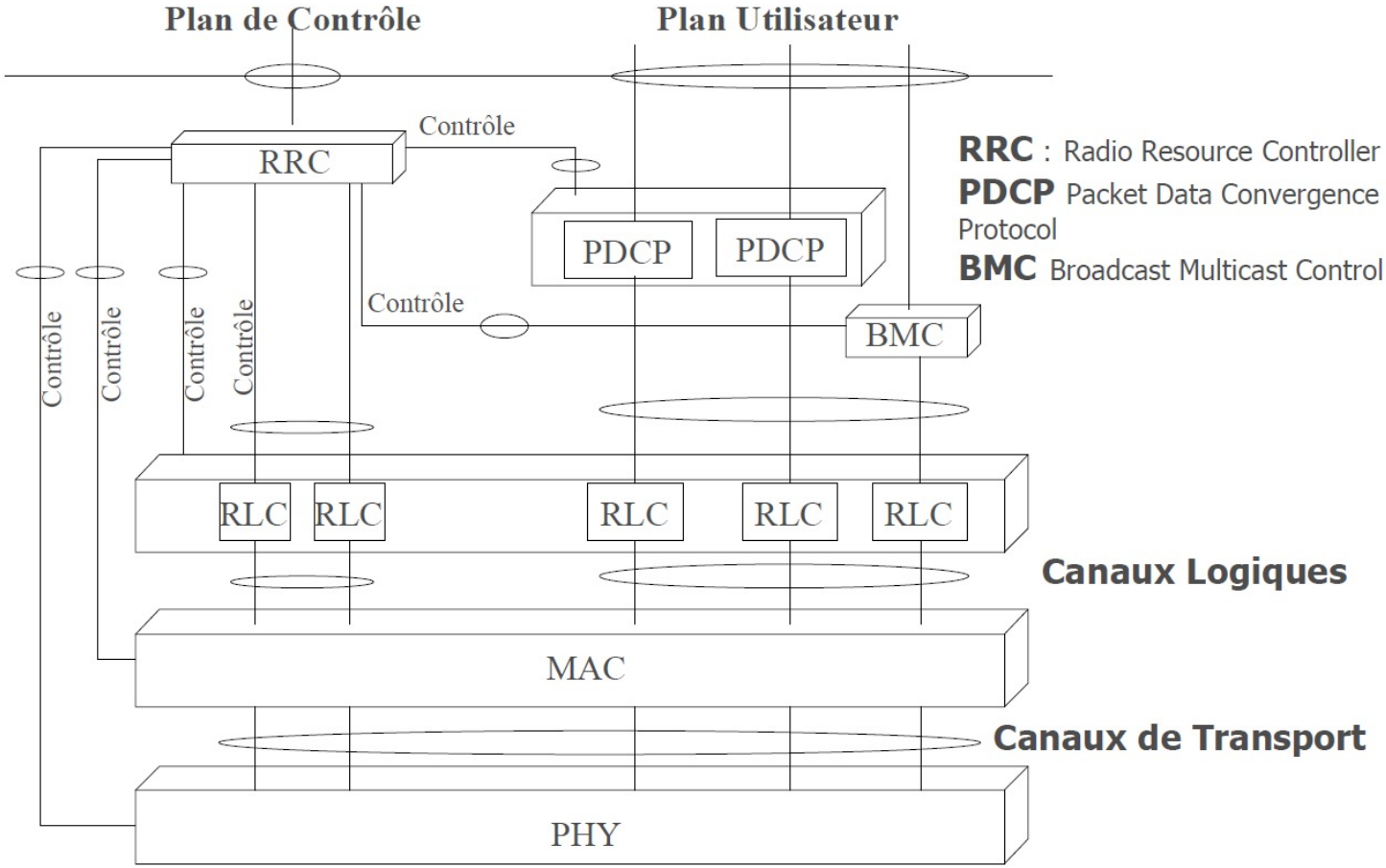
** Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller and Valtteri Niem, LTE Security, John Wiley & Sons, 2011*

- Confidentialité: f8 et Intégrité : f9
- **Implémentations:**

  UEA1 and UIA1 basés sur l'algorithme KASUMI (bloc 64, clé 128)

  UEA2 and UIA2 basés sur l'algorithme SNOW3G (flot 32, clé 128)

Confidentialité et intégrité



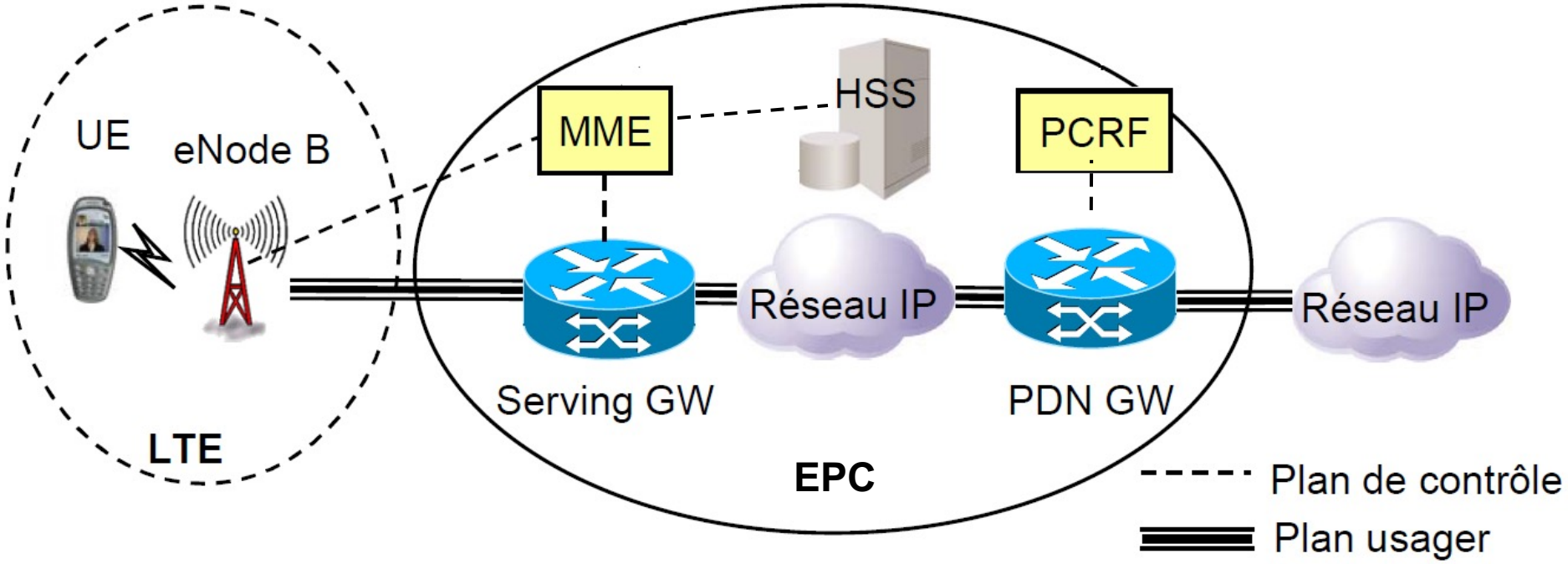
Intégrité au niveau RRC
Chiffrement au niveau RLC (non transparent) ou MAC (transparent)

Pas d'intégrité !
Chiffrement au niveau RLC (non transparent) ou MAC (transparent)

* A. BEYLOT, Architecture Protocolaire de l'UMTS cours UMTS, ENSEEIHT, Toulouse

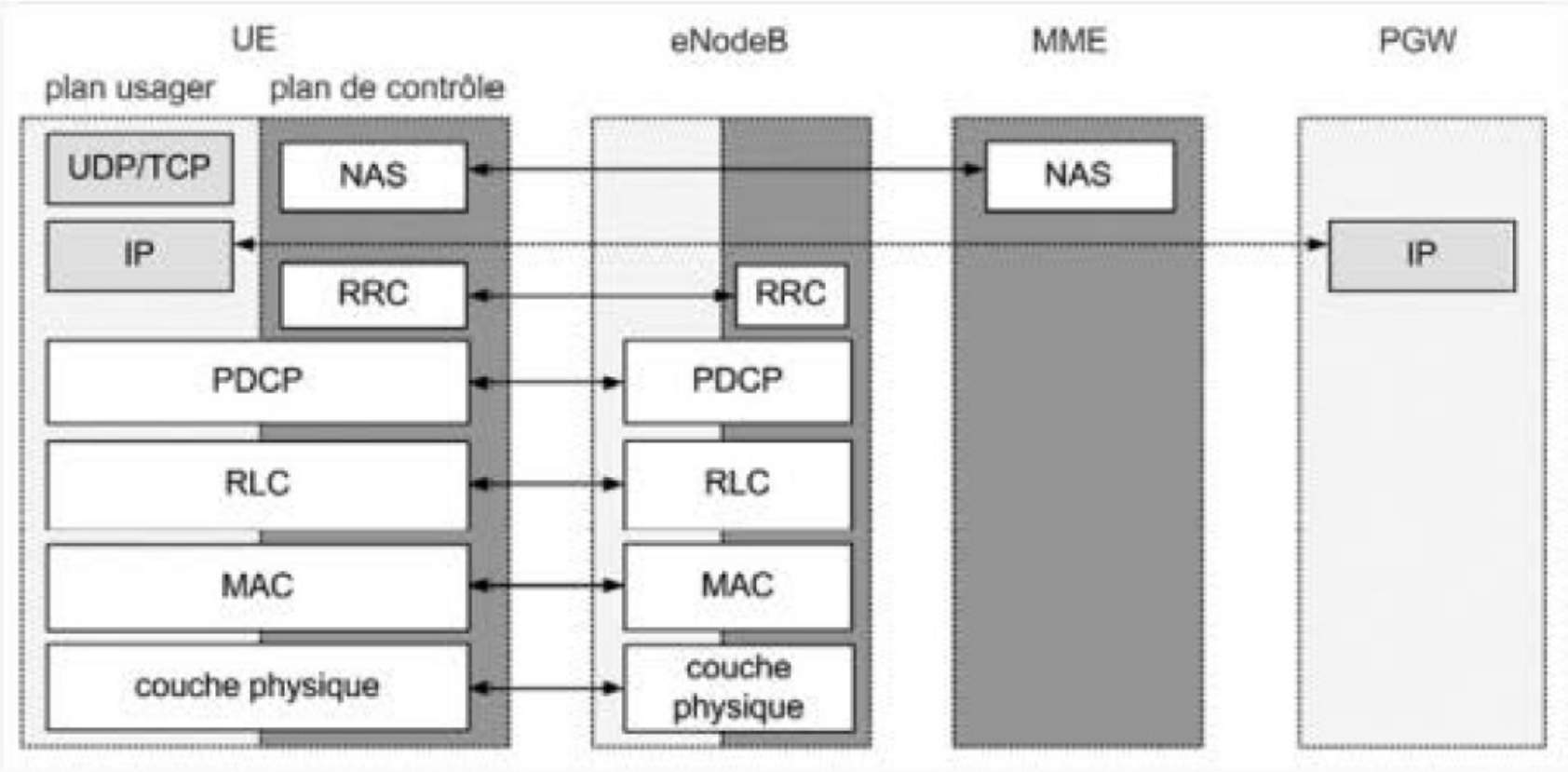
Réseaux de quatrième génération

Architecture Physique



* EFORT, LTE + SAE = EPS Principes et Architecture(http://www.efort.com)

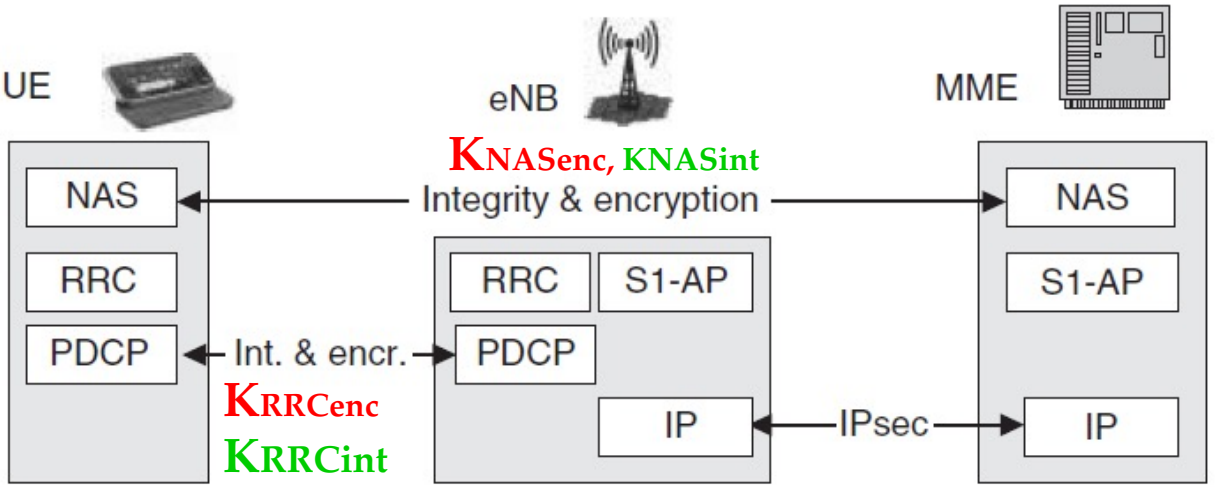
Architecture protocolaire



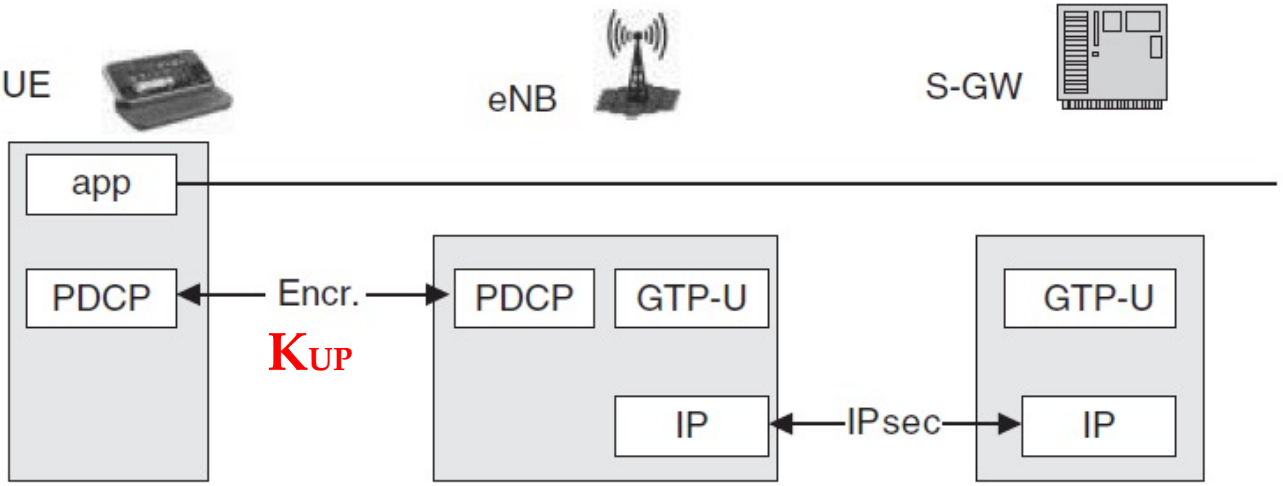
* Y. Bouguen, É. Hardouin, F. Wolff, LT, E et les reseaux 4G, EYROLLES, 2012,

Sécurité 4G: Apreçu

Plan Contrôle



Plan Usager



** Adaptée de: D.F., G. Horn, W.Di. Moeller and V. Niem, LTE Security, John Wiley & Sons, 2011*

Sécurité 4G : Axes de sécurité

- **Confidentialité de l'identité de l'abonné:** Id temporaire GUTI généré par le MME lors de l'enregistrement initial (= GUMMEI + M-TMSI)

- **Confidentialité des données de l'usager et de la signalisation:**
  - Chiffrement des données de l'usager entre l'UE et eNodeB
  - Chiffrement des données de signalisation RRC entre l'UE et eNodeB
  - Chiffrement de la signalisation NAS entre l'UE et le MME

- **Intégrité des données de signalisation**
  - Appliquée sur tous les échanges sauf les messages échangés avant l'activation de la sécurité: (Attach Request, Identity Request, RRC Connection Request, RRC Connection Setup, etc.)

- **Pas d'intégrité des données du plan usager**
  - Peut être réalisée par les couches supérieures Ipsec, etc.

Authentification et génération de clés

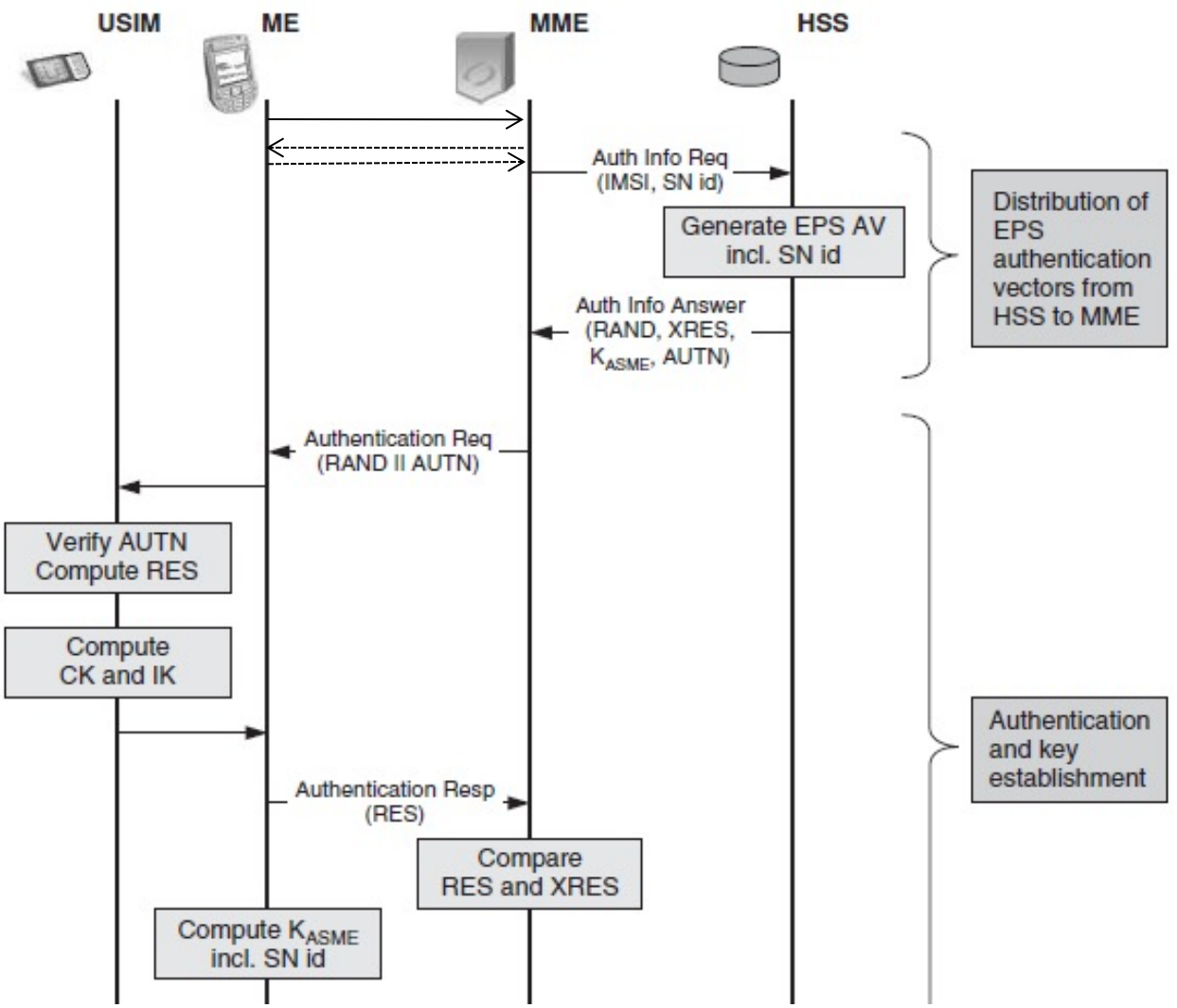
Très similaire à l'authentification UMTS:

- Clé secrète K (USIM et Auc)
- Authentification mutuelle
- Des clés intermédiaires CK et IK sont calculées par l'AuC et 'USIM

Différences:

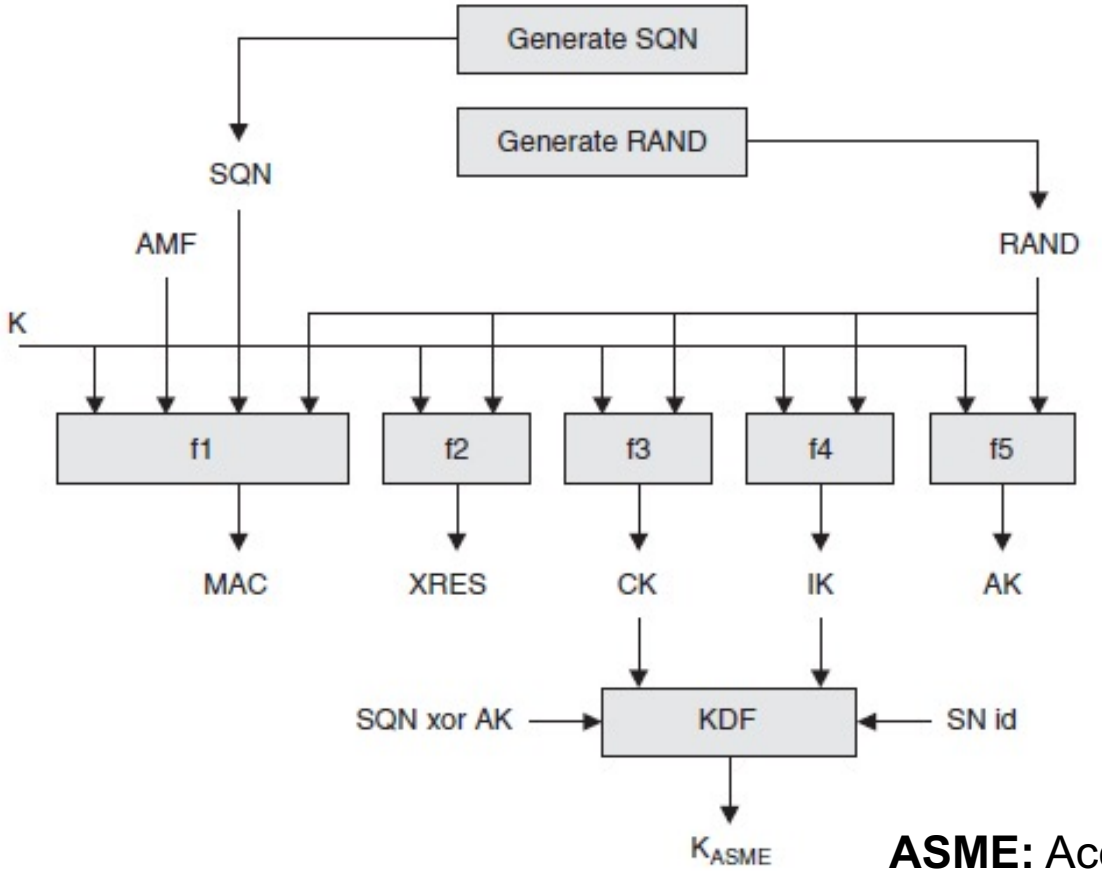
- La hiérarchie des clés: elle est constituée de plusieurs niveaux intermédiaires (CK/ IK, K_ASME et K_eNB (voir slide suivant)
- Chiffrement UE <--> l'eNodeB et UE <--> MME (protection de l'enodeB)
- Nouvelle dérivation des clés lors d'un handover entre deux eNodeB
- Un seul domaine ce qui évite la double authentification
- Nouveaux algorithmes de chiffrement et d'intégrité
- Chiffrement des données au niveau de la couche PDCP

Authentification et génération de clés



** Adaptée de: D.F., G. Horn, W.Di. Moeller and V. Niem, LTE Security, John Wiley & Sons, 2011*

Authentification et génération de clés (HSS/AUC)



AUTN := SQN xor AK || AMF || MAC

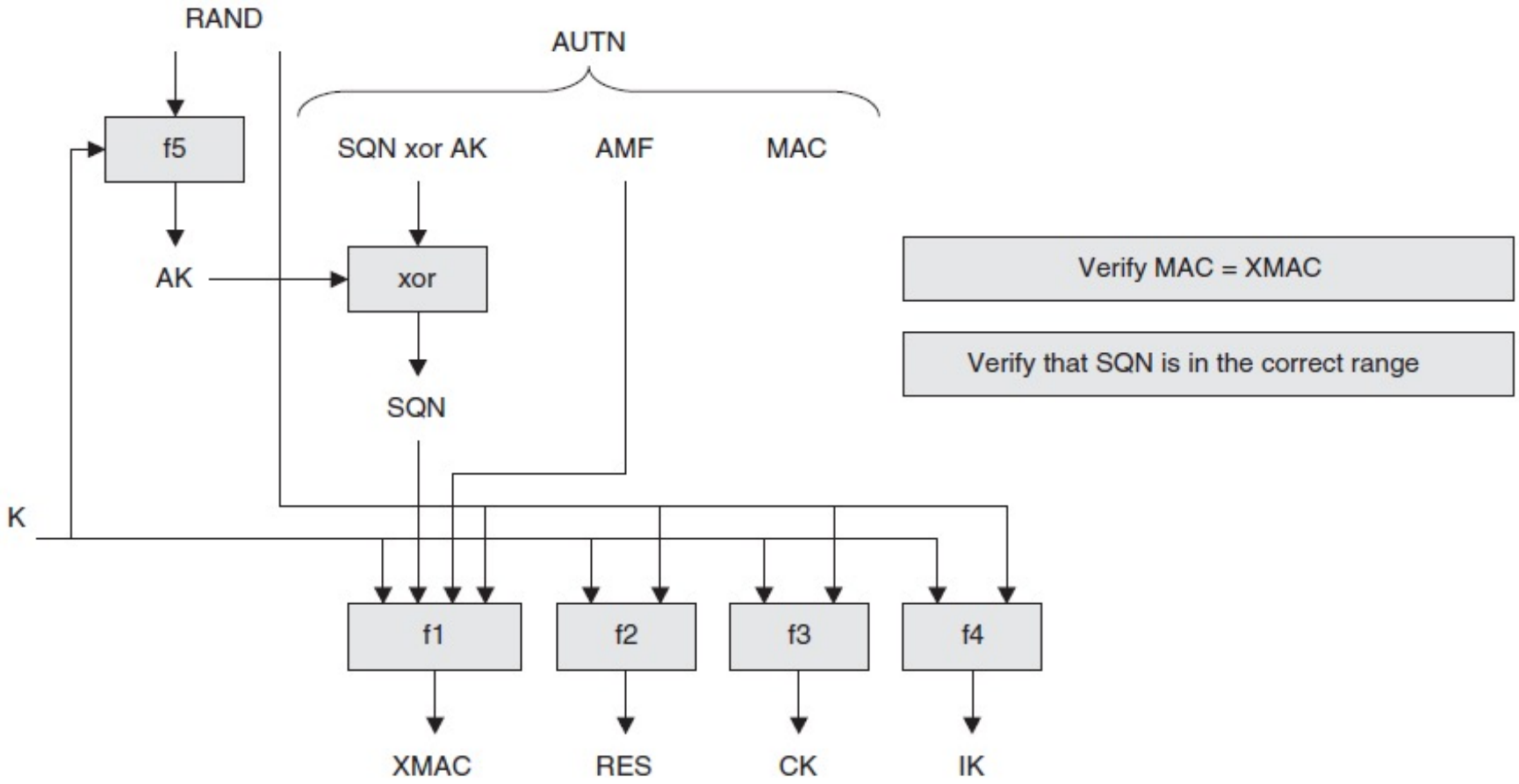
UMTS AV := RAND || XRES || CK || IK || AUTN

EPS AV := RAND || XRES || K_{ASME} || AUTN

ASME: Access Security Management Entity

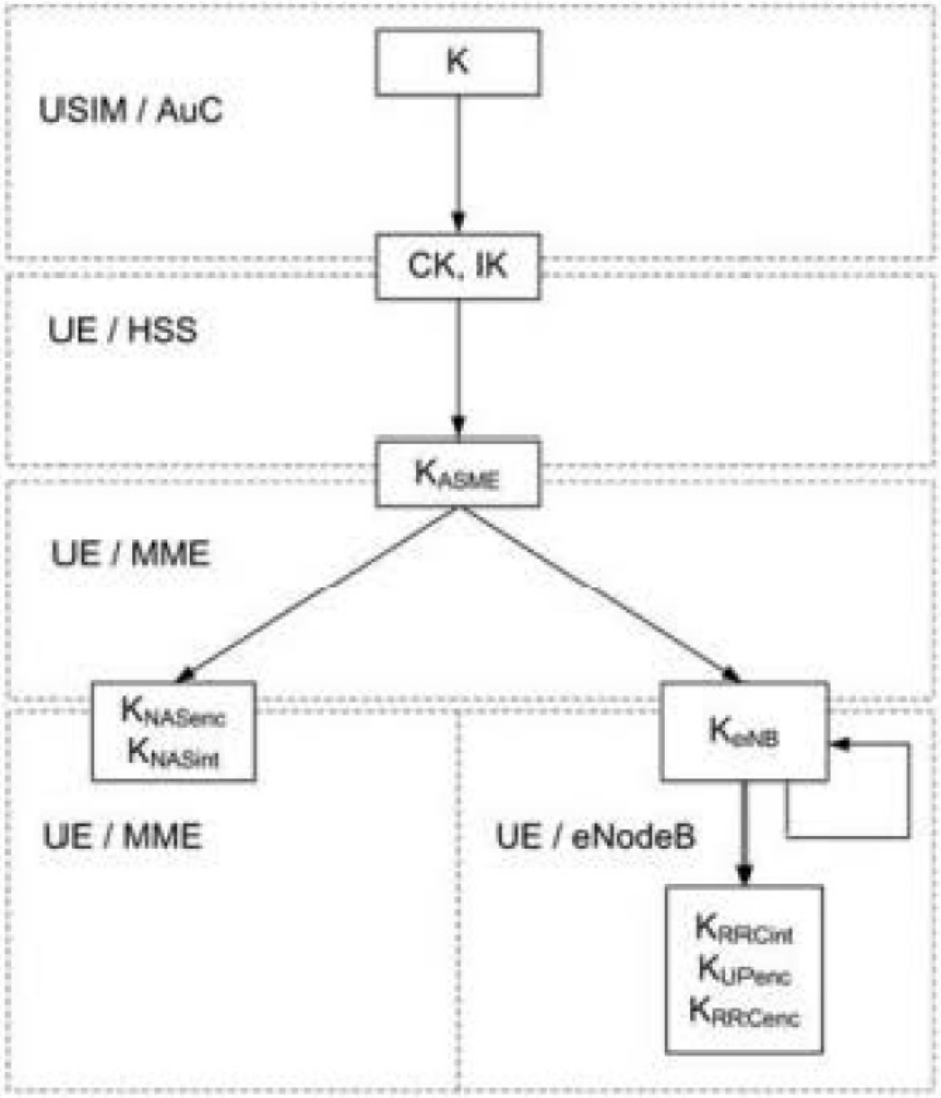
** Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller and Valtteri Niem, LTE Security, John Wiley & Sons, 2011*

Authentification et génération de clés (UE)



** Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller and Valtteri Niem, LTE Security, John Wiley & Sons, 2011*

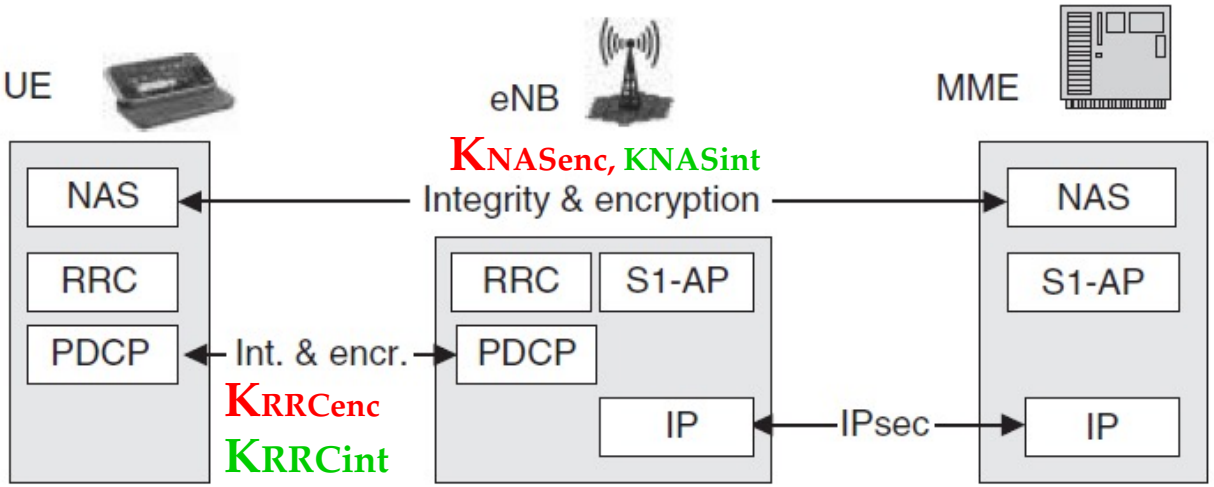
Hiéarchie des clés



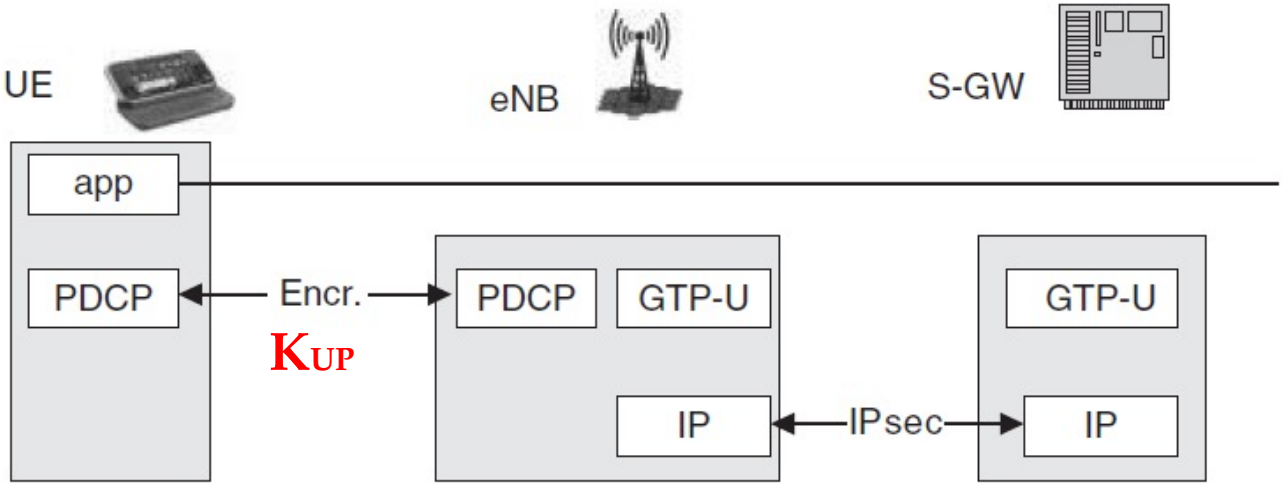
* Y. Bouguen, É. Hardouin, F. Wolff, LTE et les reseaux 4G, EYROLLES, 2012

Utilisation des clés

Plan Contrôle



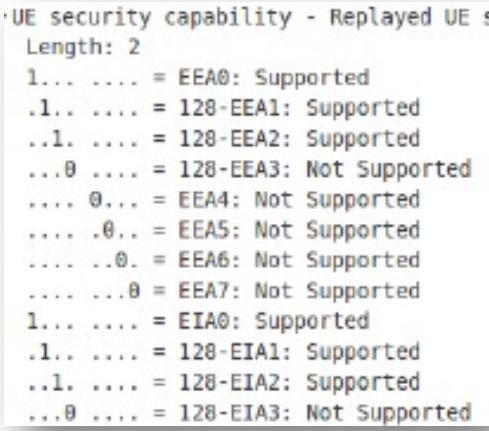
Plan Usager



** Adaptée de: D.F., G. Horn, W.Di. Moeller and V. Niem, LTE Security, John Wiley & Sons, 2011*

Algorithmes de chiffrement et d'intégrité

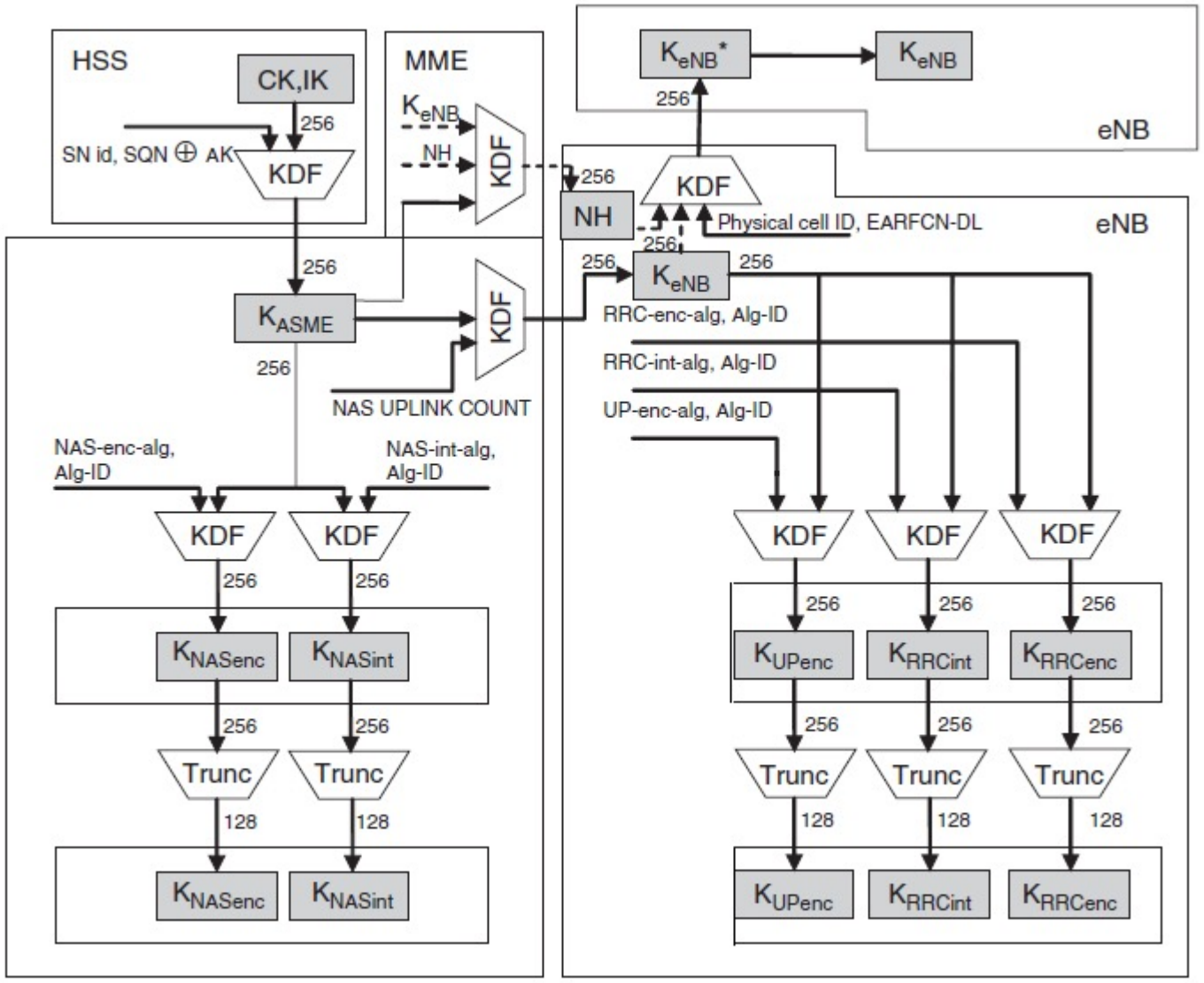
- Similaire aux réseaux UMTS (confidentialité + intégrité)
  - EEA1/EIA1 – basé sur SNOW 3G
  - EEA2/EIA2 – basé sur AES (USA)
  - EEA3/EIA3 – basé sur ZUC (China)



- MME choisit les algorithmes sur la base de ses capacités et de celles de l'UE (Possibilité de choisir des algorithmes différents conf / intég)

- K_{eNb} et K_{asme} sur 256 bits
- Toutes les clés de chiffrement et d'intégrité sont générées sur 256 bits et tronquées sur 128 bits (possibilité de passage à 256 bits)

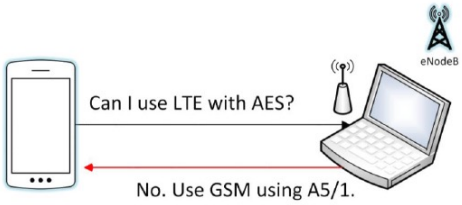
Algorithmes de chiffrement et d'intégrité



* *Adaptée de: D.F., G. Horn, W.Di. Moeller and V. Niem, LTE Security, John Wiley & Sons, 2011*

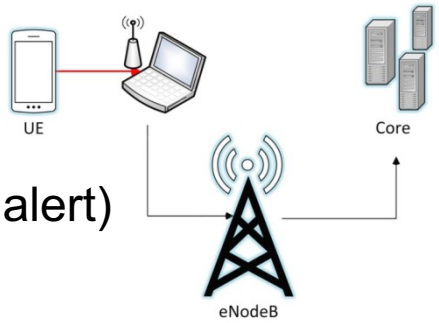
Quelques attaques contre les réseaux LTE

- **EnodeB malveillant (Rogue base stations)**



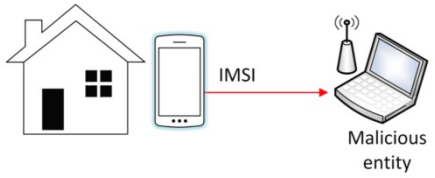
  - **Forcer le passage à la 2G/3G**

    (attaque par renégociation, solution: Use LTE only' option)



  - **Interception des communications**

    (attaque par renégociation, unencrypted connection alert)



  - **Interception de l'IMEI et de l'IMSI**

    Mise à jour de l'identité temporaire

Aperçu sur les évolutions dans les réseaux de cinquième génération

Merci !