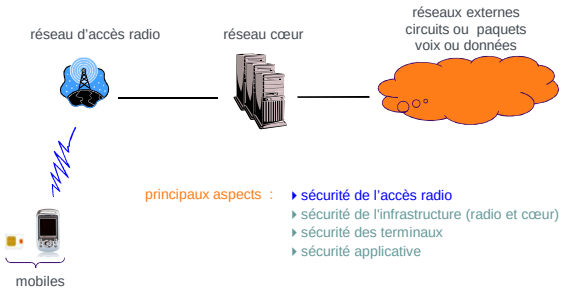
Cryptographie dans les réseaux radiomobiles

Henri Gilbert
resp. du laboratoire de cryptographie de l'ANSSI
henri.gilbert@ssi.gouv.fr

10 février 2016

sommaire

besoins de sécurité des systèmes mobiles
GSM / UMTS / EPS



principaux aspects :
- sécurité de l'accès radio
- sécurité de l'infrastructure (radio et cœur)
- sécurité des terminaux
- sécurité applicative

besoins de sécurité liés à l'accès radio (1)

menaces	contre-mesures
usurpation d'identité (clonage, rejeu)	authentification forte de l'abonné
détournement de communication (hijacking)	intégrité de la signalisation
écoute depuis un équipement passif	chiffrement (limité ou non à la voie radio)

besoins de sécurité liés à l'accès radio (2)

menaces	contre-mesures
usurpation d'identité (clonage, rejeu)	authentification de l'abonné
détournement de communication (hijacking)	intégrité de la signalisation
écoute depuis un équipement passif	chiffrement limité ou non à la voie radio
écoute depuis une fausse station radio (attaques dans le milieu)	- authentification mutuelle (protection partielle) - chiffrement systématique (imposé par le mobile) - indicateur de chiffrement
localisation / filature radio	identités temporaires et chiffrement

besoins de sécurité liés à l'accès radio (3)

menaces	contre-mesures
usurpation d'identité (clonage, rejeu)	authentification de l'abonné
détournement de communication (hijacking)	intégrité de la signalisation
écoute depuis un équipement passif	chiffrement limité ou non à la voie radio
écoute depuis une fausse station radio (attaques dans le milieu)	- authentification mutuelle (protection partielle) - chiffrement systématique (imposé par le mobile) - indicateur de chiffrement
localisation / filature radio	identités temporaires et chiffrement
vol de la carte (U)SIM vol du terminal abonnements fantômes	code PIN listes noires d'IMEI organisationnelles

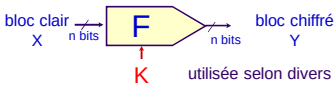
principaux mécanismes cryptographiques (rappel)

	Cryptographie symétrique	Cryptographie asymétrique
Confidentialité	chiffrement symétrique	chiffrement asymétrique
Authentification d'entité	authentification	identification
Authentification de message	code d'authentification de message (MAC)	signature
Echange de clé	-	schéma d'échange de clé

algorithmes symétriques (rappel)

- algorithmes par blocs (ex : AES)

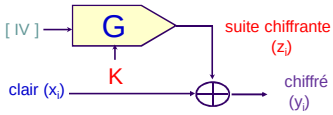
à la clé K est associée une fonction bijective F_K



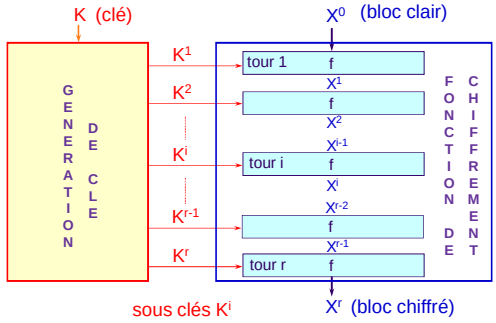
utilisée selon divers modes opératoires

- algorithmes à flot (ex : GSM A5/1)

à la clé K est associée une suite binaire (z_i)



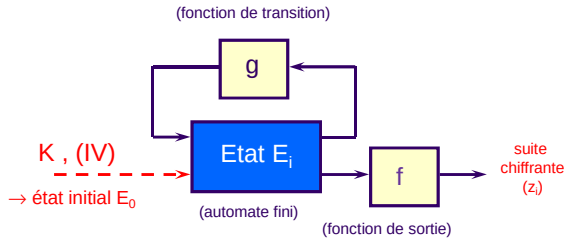
structure des algorithmes par blocs (rappel)



exemples d'algorithmes par blocs

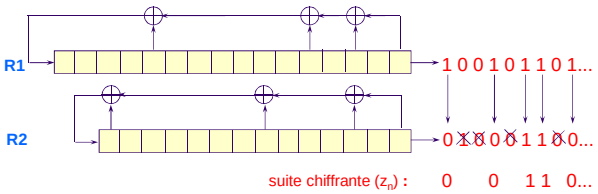
algorithme	taille de clé	taille des blocs	origine	utilisé dans
DES 3DES	56 112	64 64	IBM	nombreux produits
RC2 RC6	40-256 128-256	64 128	Rivest RSA Labs	S/MIME
IDEA	128	64	Massey Lai	PGP
MISTY KASUMI	128 128	64 64	Matsui 3GPP	UMTS
AES (Rindael)	128-256	128	Daemen Rijmen	remplace graduellement DES

structure des algorithmes à flot (rappel)



exemple : shrinking generator [Coppersmith et al.]

Utilise deux registres à décalage linéaires à rétroaction linéaire R1 et R2



- seuls les bits de R2 tels que le bit correspondant de R1 vaut 1 sont sélectionnés
- longueurs recommandées : |R1| et |R2| ≥ 128
- les polynômes caractéristiques de R1 et R2 doivent être primitifs et non creux

exemples d'algorithmes à flot

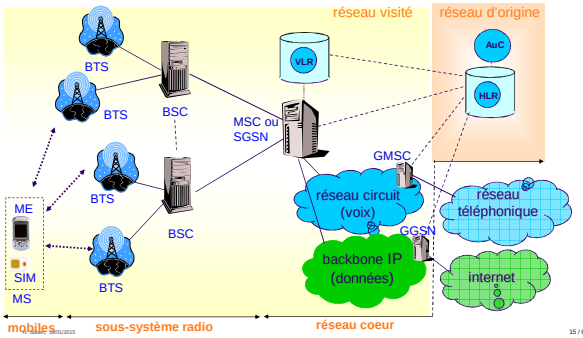
algorithme	taille clé / IV	origine	utilisé dans
RC4	40-256 / -	RSA-Labs	SSL
A5/1 GEA2	64 / 22 64 / 32	ETSI ETSI	GSM GPRS
SEAL SCREAM Shrinking Generator	128 / 32 128 / 128 ≥ 128 /-	IBM	
E0	128 / -		Bluetooth
SNOW 2.0 SNOW 3G	128 / 128 128 / 128	U. Lund 3GPP	 UMTS

+ 7 algorithmes à flot retenus à l'issue de la compétition européenne eSTREAM

sommaire

architecture du système GSM

MS : Mobile Station
BTS : Base Transceiver Station
BSC : Base Station Controller
MSC : Mobile Switching Center
SGSN : Serving GPRS Support Node
GMSC : Gateway MSC
VLR : Visited Location Register
HLR : Home Location Register
AuC : Authentication Center



GSM : principales fonctions de sécurité

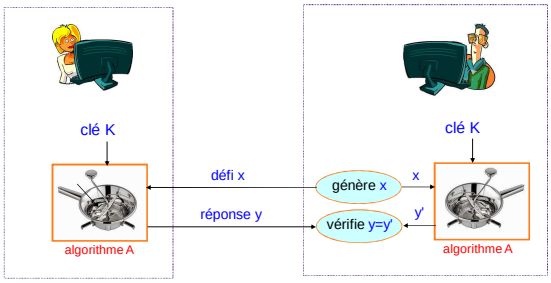
- authentification de l'identité de l'abonné
  - assure le contrôle d'accès au réseau, permet d'éviter la fraude
- confidentialité (chiffrement limité à l'interface radio)
  - trafic (voix, données)
  - signalisation
- confidentialité de l'identité de l'abonné (anonymat)
  - protège l'abonné contre la localisation / filature depuis un scanner radio

GSM : anonymat

IMSI = International Mobile Subscriber Identity = identité permanente
TMSI = Temporary Mobile Subscriber Identity = pseudonyme fréquemment renouvelé

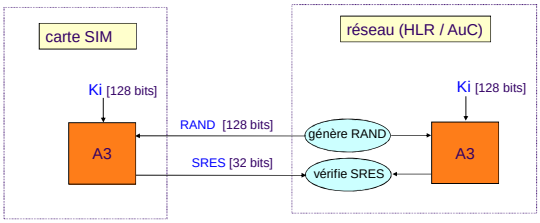
- première communication après mise en service
  - le mobile envoie au réseau son IMSI en clair
  - le réseau passe en mode chiffré
  - le réseau envoie au mobile une première valeur de TMSI
- communications ultérieures
  - le mobile envoie au réseau son TMSI en clair
  - la valeur du TMSI est renouvelée après passage en chiffrement lors des mises à jour de localisation
  - repli en cas de perte du TMSI : envoi de l'IMSI en clair
- pas de protection contre les attaques actives
  - depuis un "IMSI catcher" (fausse BTS)

authentification symétrique (principe)



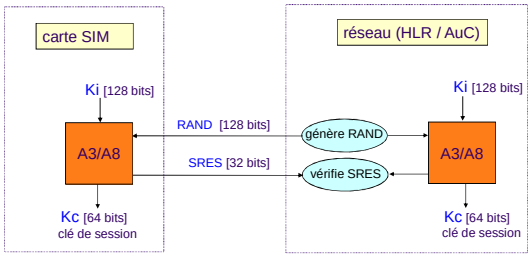
- non rejeu : les anciennes réponses ne permettent pas de répondre à de nouveaux défis
- "non forgeabilité" : observer N échanges ne permet pas de prédire une nouvelle réponse

authentification GSM (1)



- fondée sur le partage d'une clé individuelle Ki entre le SIM et l'AuC
- effectuée au début de chaque session : communications, mises à jour de localisation

authentification GSM (2)

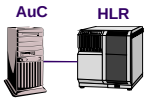


- fondée sur le partage d'une clé individuelle Ki entre le SIM et l'AuC
- effectuée au début de chaque session : communications, mises à jour de localisation
- combinée avec le renouvellement de la clé de session Kc (GSM circuit) ou Kc* (GPRS)
- les algorithmes A3 et A8 ne sont pas normalisés

modules de sécurité : SIM et AuC

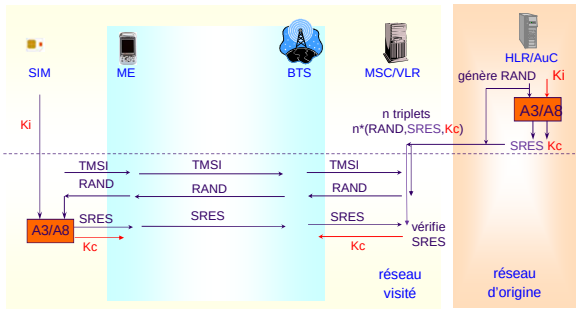
- **SIM (Subscriber Identity Module)**
  - personnalisée avant mise en service
  - contient Ki et l'algorithme A3/A8
  - sécurité physique et logique (OS)
  - protégée contre le vol au moyen d'un code PIN vérifié dans la carte
- **AuC (Authentication Center)**
  - rattaché au HLR
  - options : stockage ou reconstitution des clés Ki
  - génération de triplets (RAND, SRES, KC)

Ki + A3/A8

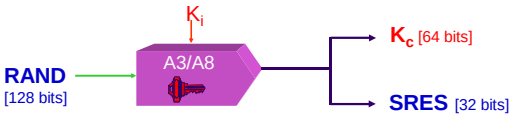


Clés Ki + A3/A8

authentification GSM : détail des échanges



algorithme A3/A8 : propriétés requises



- non forgeabilité, imprédictibilité : l'observation de n sorties (Kc, SRES) correspondant à des entrées RAND connues ou choisies ne doit pas permettre de calculer la clé Ki ou de prédire une sortie correspondant à une nouvelle valeur RAND.
- en particulier, résistance aux méthodes d'attaque connues

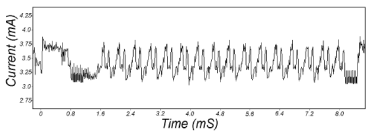
  cryptanalyse linéaire, cryptanalyse différentielle, attaques par collisions, etc.
- séparation cryptographique

  la donnée de SRES ne doit fournir aucune information sur Kc (et inversement)
- l'implantation de A3/A8 doit résister aux attaques par canaux auxiliaires

attaques par canaux auxiliaires

- principe : mise en défaut du modèle de fonctionnement en boîte noire
  - timing attacks, erreurs provoquées
  - rayonnement électromagnétique
  - mesures de consommation électrique

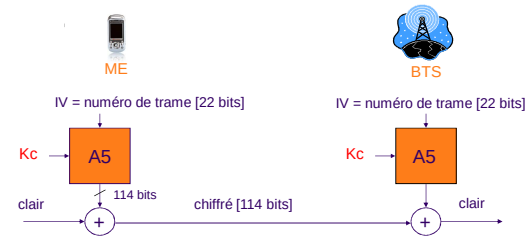
    corrélation entre la consommation électrique à certains instants et la valeur de données dépendant d'un nombre restreint de bits de clé
    - SPA = Simple Power Analysis
    - DPA = Differential Power Analysis



algorithmes A3/A8

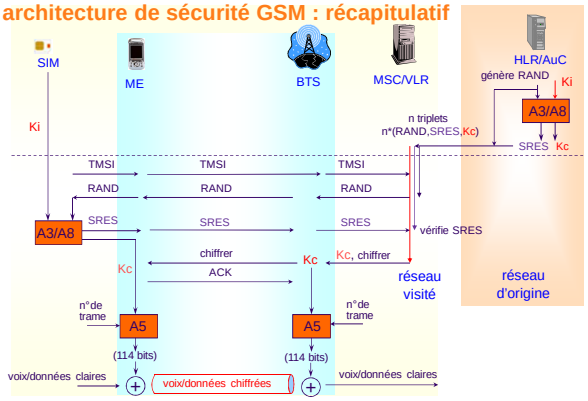
- COMP128 : un exemple à ne pas suivre
  - distribué à titre d'exemple par l'association des opérateurs GSM jusqu'en 1998
  - vulnérable à une attaque nécessitant quelques dizaines de milliers de défis/réponses
    ⇒ une carte SIM COMP128 peut être "clonée" par son détenteur
  - désormais remplacé par un autre algorithme par la plupart des opérateurs
- autres algorithmes A3/A8
  - COMP128-2 : distribué par l'association des opérateurs GSM, non publié, peu utilisé
  - MILENAGE-2G : transposition au GSM de l'algorithme 3G MILENAGE
  - algorithmes spécifiques (non publiés) développés par certains opérateurs

chiffrement GSM / circuit



- le chiffrement porte sur l'ensemble du trafic et de la signalisation
- il repose sur l'emploi de Kc et d'un algorithme de chiffrement à flot normalisé (A5)
- place paradoxale dans les traitements radio : codage correcteur / chiffrement / modulation

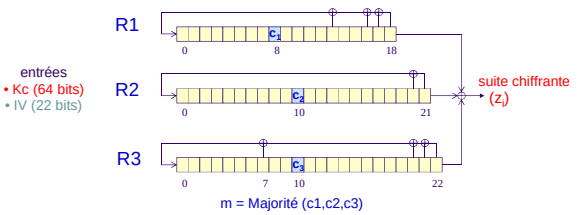
architecture de sécurité GSM : récapitulatif



algorithmes A5

- A5/1
  - massivement déployé
  - usure graduelle : A5/1 n'offre pas une protection absolue de la confidentialité
    - meilleure attaque connue : compromis temps/mémoire/données [BBK03]
    - démonstrations récentes d'écoute différée [CCC]
- A5/2
  - algorithme export
  - utilisé dans un nombre restreint de réseaux
  - des attaques très réalistes ont été publiées
- A5/3 et A5/4
  - longueurs de clé : 64 bits et 128 bits ; spécifiés et publiés en 2002
  - dérivés de l'algorithme par blocs 3G KASUMI, pas d'attaques connues
  - déploiement relativement lent
- négociation de l'algorithme A5 en début de communication
  - le terminal fournit sa liste d'algorithmes, qui contient obligatoirement A5/1
  - le réseau indique l'algorithme choisi lors du passage en chiffrement
  - absence de séparation cryptographique entre les algorithmes
    - attaque potentielle par fausse BTS : passage en chiffrement A5/2 afin de reconstituer Kc

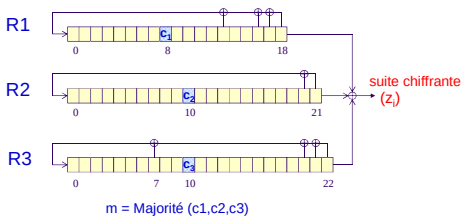
algorithme de chiffrement A5/1



fonctionnement : 4 étapes à chaque trame

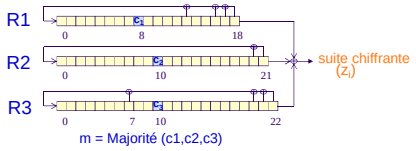
- (1) chargement de Kc (64 bits) et (2) chargement de IV (22 bits) dans R1, R2, R3
  avancée régulière de R1, R2, R3 (XOR du bit injecté avec les 3 bits de rebouclage)
- (3) 100 « tours à vide » et (4) production de 2x114 bits chiffrants
  à chaque coup d'horloge, seuls les registres Ri tels que c_i=m avancent

propriétés de A5/1



- automate à états : seulement 2^{64} états initiaux ; diminution (lente) du nombre d'états possibles
- chargement linéaire : faiblesse potentielle
- avancées irrégulières : évite certaines faiblesses des générateurs à combinaison de registres
- fonction de sortie linéaire ⇒ non corrélation avec un ou deux des registres R1, R2, R3

A5/1 : meilleures attaques connues

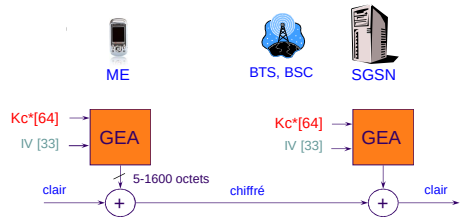


existence d'attaques « à clair connu » plus efficaces que la recherche exhaustive de Kc

⇒ érosion de la protection offerte par A5/1

- connaissance de n [≈ 64] bits de clair consécutifs [Golic ; Pornin-Stern] complexité ≈2^{42} systèmes linéaire
- connaissance de plusieurs trames de clair et utilisation de compromis temps/(mémoire)/données
  [Biryukov-Shamir-Wagner ; Biham-Dunkelman ; Barkan-Biham-Keller 2003 : à partir du seul chiffré]
- connaissance statistique des [40] premiers bits de clair de N [≈60000] trames [Ekdahl, Johansson]

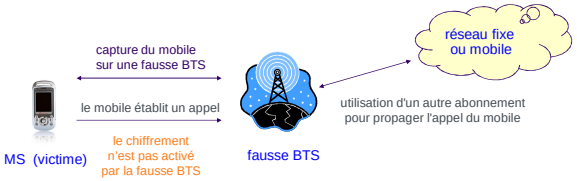
chiffrement GSM / paquets (GPRS)



- le chiffrement porte sur les unités de données du protocole MS-SGSN de niveau 2
- plusieurs algorithmes GEA (GPRS encryption algorithm) ont été normalisés :
  - GEA 1 et GEA 2 algorithmes initiaux (choix conseillé : GEA2)
  - GEA 3 et GEA 4 algorithmes publics fondés sur l'algorithme 3G KASUMI

limites de la sécurité du système GSM (1)

- le chiffrement s'arrête à la BTS ⇒ vulnérabilité de l'interface BTS-BSC
  - les échanges de signalisation dans l'infrastructure fixe ne sont pas chiffrés
- chiffrement laissé à l'initiative du réseau + pas d'authentification du réseau par le mobile
  - risque d'écoute (1) : à l'aide d'une fausse station de base



- contremesure dans certains terminaux : indicateur de chiffrement

limites de la sécurité du système GSM (2)

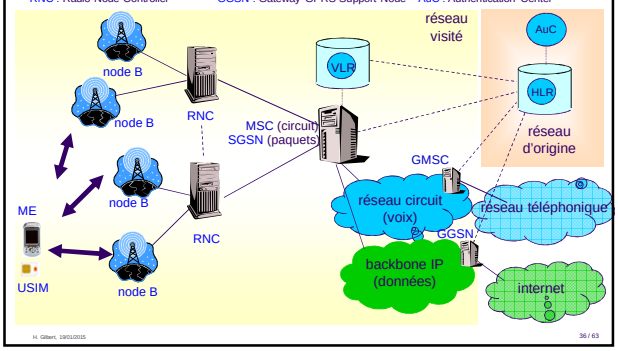
- le chiffrement s'arrête à la BTS ⇒ vulnérabilité de l'interface BTS-BSC
  - les échanges de signalisation dans l'infrastructure fixe ne sont pas chiffrés
- chiffrement laissé à l'initiative du réseau + pas d'authentification du réseau par le mobile
  - risque d'écoute (1) : à l'aide d'une fausse station de base
  - contremesure dans certains terminaux : indicateur de chiffrement
- pas de séparation cryptographique entre les algorithmes de chiffrement (A5/1 et A5/2)
  - risque d'écoute (2) : à l'aide d'un équipement en coupure capable de décrypter A5/2
  - contremesures : abandon de A5/2 (en cours), séparation cryptographique (long terme)
- érosion de la confidentialité assurée par l'algorithme A5/1 (cf supra)
  - risque d'écoute (3) : à l'aide d'un équipement passif capable de décrypter A5/1 [BBK03]
  - contremesure pour les communications GSM confidentielles : surchiffrement
- pas de protection contre le rejeu d'anciens défis A3/A8
  - risque de déchiffrement a posteriori de communications chiffrées enregistrées par un attaquant
    - par exemple en cas de vol ultérieur de la carte SIM par l'attaquant

sommaire

- introduction
  - besoins de sécurité liés à l'accès radio (tous systèmes)
- sécurité des systèmes 2G : (GSM / circuits et GSM / paquets : GPRS)
  - architecture de sécurité
  - authentification et distribution de clés : algorithmes A3/A8
  - chiffrement : algorithmes A5 et GEA
- écurité des systèmes 3G (UMTS : universal mobile telecommunications system)
  - architecture de sécurité
  - authentification et distribution de clé :
    l'exemple d'algorithme MILENAGE, fondé sur l'AES
  - chiffrement et intégrité : algorithmes KASUMI et SNOW 3G
    - algorithme par blocs KASUMI, modes f8 et f9
    - algorithme de repli SNOW 3G
- sécurité 4G – esquisse (EPS - evolved packet system)

architecture du système UMTS

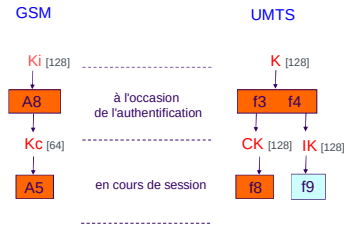
USIM : UMTS Subs. Ident. Module
MS : Mobile Station
RNC : Radio Node Controller
SGSN : Serving GPRS Support Node
MSC : Mobile Switching Center
GGSN : Gateway GPRS Support Node
VLR : Visited Location Register
HLR : Home Location Register
AuC : Authentication Center



sécurité UMTS : améliorations par rapport à GSM

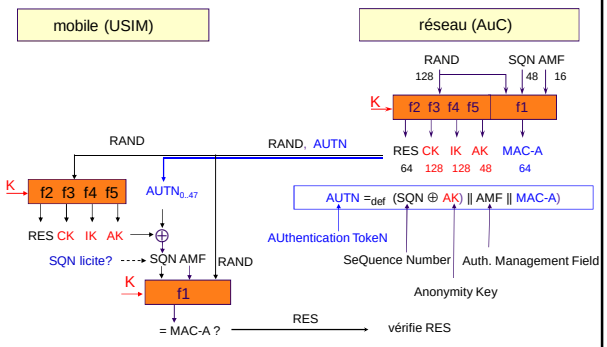
- nouveau mécanisme d'authentification / établissement de clés (fonctions f1-f5)
  - authentification mutuelle entre réseau et la carte USIM
  - mécanisme anti-rejeu des valeurs d'authentification dans la carte USIM
- nouveaux algorithmes de chiffrement (fonction f8)
  - le chiffrement va jusqu'au cœur du sous-système radio
  - algorithmes KASUMI et SNOW 3G, utilisent des clés de 128 bits
- intégrité des messages de signalisation (fonction f9)
  - un MAC (code d'authentification de messages) est appliqué à la signalisation
  - notamment au message obligatoire d'établissement du contexte de sécurité

UMTS : hiérarchie des clés

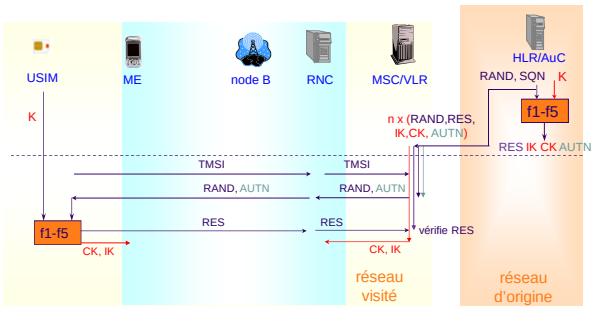


- Ki et K : clés d'authentification et de distribution de clés de l'abonné
- Kc et CK : clés de session : chiffrement A5 et f8
- IK : clé d'intégrité f9 (MAC)

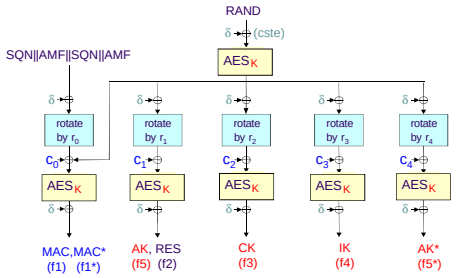
authentification UMTS (AKA : auth & key agreement)



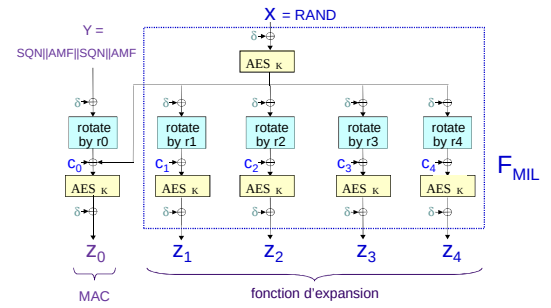
authentification UMTS : détail des échanges



MILENAGE : un exemple d'algorithme AKA fondé sur l'AES

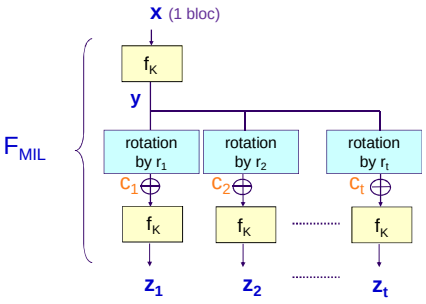


sécurité de MILENAGE

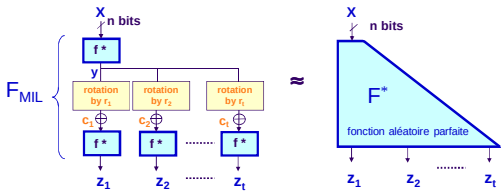


- objectifs : - sécurité de chaque fonction + séparation cryptographique entre fonctions
  - pas d'attaque réaliste de complexité << 2^{128}
  - pas de "distingueur" de complexité << 2^{64}

fonction d'expansion de MILENAGE

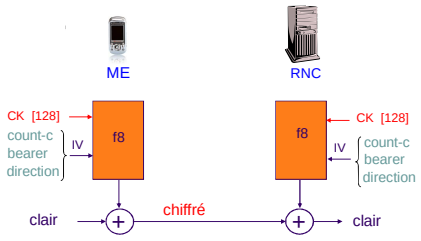


sécurité de la fonction d'expansion de MILENAGE

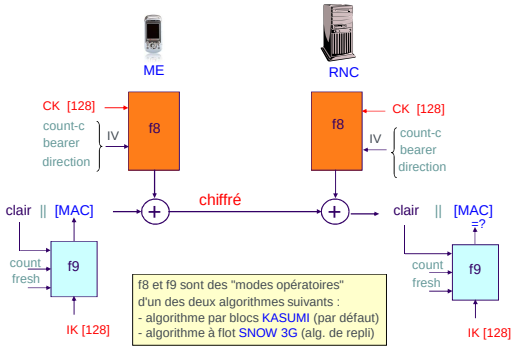


Si les constantes ci et ri sont convenablement choisies et si q est suffisamment petit devant $2^{n/2}$, **aucun test utilisant q questions/réponses ne permet de distinguer F_{MIL} de F*** avec un "avantage" significatif.

chiffrement UMTS (chiffrement f8)

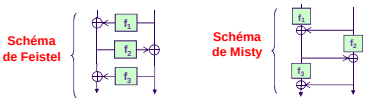


intégrité UMTS (code d'authentification de messages f9)

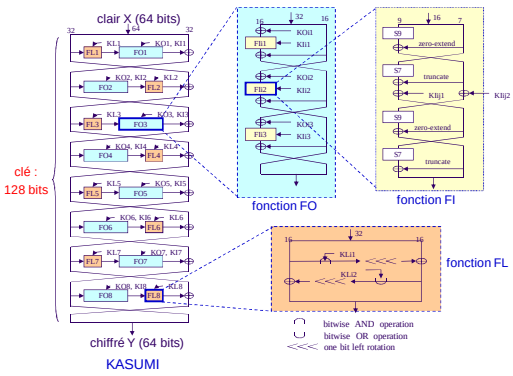


chiffrement et intégrité UMTS : l'algorithme par blocs KASUMI

- taille des blocs = 64 bits ; taille des clés = 128 bits
- dérivé de l'algorithme MISTY1 [Matui et al.]
- opérations élémentaires :
  - **boîte S7 :** équivalente à $x \rightarrow x^{81}$ dans GF(128) $\Rightarrow$ 7 équations de degré 3
  - **boîte S9 :** équivalente à $x \rightarrow x^{5}$ dans GF(512) $\Rightarrow$ 9 équations de degré 2
  - **opérations linéaires :** $\oplus$ (ou exclusif), <<< (rotation)
- schéma de génération de sous-clés clés très simple (affine modulo 2)
- structure emboîtée
  - **fonction F (64 bits)** = 8 appels à la fonction FO - **schéma de Feistel**
  - **fonction FO (32 bits)** = 3 appels à la fonction FI - **schéma de Misty**
  - **fonction FI (16 bits)** = 2 appels aux boîtes S7 et S9 - **schéma de Misty**

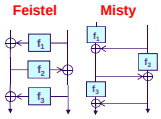


KASUMI (algorithme par blocs dérivé de MISTY)



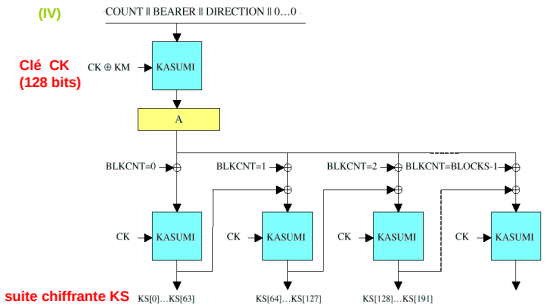
sécurité de KASUMI
résistance aux attaques différentielle et linéaires

- **définition** $DP^F = Max_{\alpha\neq 0,\ \beta} E_K \{ Pr [\Delta F(x) = \beta \mid \Delta x = \alpha] \}$
  $LP^F = Max_{\alpha,\ \beta\neq 0} E_K \{ (2 Pr [F(x) \bullet \beta = x \bullet \alpha] - 1)^2 \}$
- **théorème** [Nyberg, Knudsen, Aoki, Matsui]
  pour les schémas de Feistel et Misty à 3 étages, on a :
  $DP^{fi} \leq p$ pour i = 1 à 3 $\Rightarrow$ $DP^F \leq p^2$
  $LP^{fi} \leq p$ pour i = 1 à 3 $\Rightarrow$ $LP^F \leq p^2$



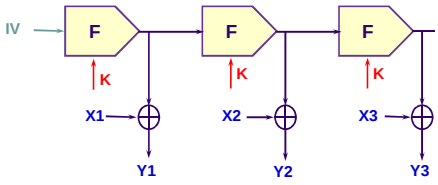
- **application à KASUMI**
  - **fonction FI :** $DP^{S7} = 2^{-6}$ et $DP^{S9} = 2^{-8}$ $\Rightarrow$ $DP^{FI} \leq 2^{-14}$
    $LP^{S7} = 2^{-6}$ et $LP^{S9} = 2^{-8}$ $\Rightarrow$ $LP^{FI} \leq 2^{-14}$
  - **fonction F0 :** $DP^{FI} \leq 2^{-14} \Rightarrow DP^{F0} \leq 2^{-28}$
    $LP^{FI} \leq 2^{-14} \Rightarrow LP^{F0} \leq 2^{-28}$
  - **fonction F (KASUMI)** : $DP^{F0} \leq 2^{-28} \Rightarrow DP^{F} \leq 2^{-56}$
    $LP^{F0} \leq 2^{-28} \Rightarrow LP^{F} \leq 2^{-56}$
- **existence d'une attaque "à clés reliées"** [DKS, janvier 2010]
  - modèle d'attaque peu réaliste : l'adversaire peut provoquer des modifications de son choix de la clé inconnue et faire chiffrer/déchiffrer des entrées de son choix
  - aucune conséquence sur la sécurité pratique de GSM et UMTS malgré la faible complexité (quelques millions d'entrées, quelques milliards d'opérations)

chiffrement (mode f8 de Kasumi)



modes opératoires (rappel)

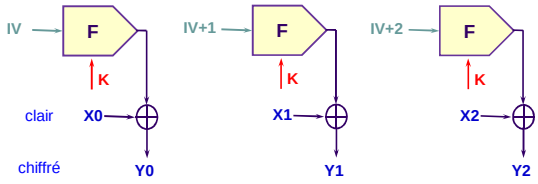
OFB (output feedback)



autre modes chiffrant : mode compteur

modes opératoires (rappel)

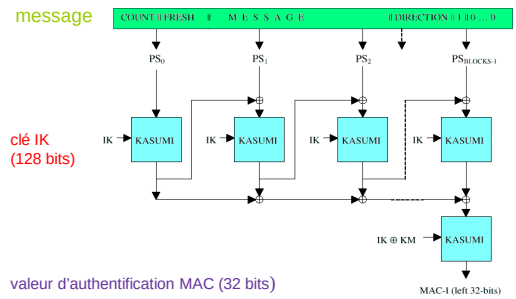
CNT (counter mode)



sécurité du mode f8

- objectifs
  - pas d'attaque réaliste de complexité << 2^{128}
  - si possible, pas de distingueur d'un générateur aléatoire ne nécessitant que 2^{32} blocs chiffrants
- avantages par rapport aux mode OFB et CNT
  - mode OFB seulement $\Rightarrow$ cycles courts potentiels
  - mode CNT seulement $\Rightarrow$ forte probabilité de propagation des collisions
- avantages du prewhitening (précalcul de A)
  - protection contre les attaques à clair connu

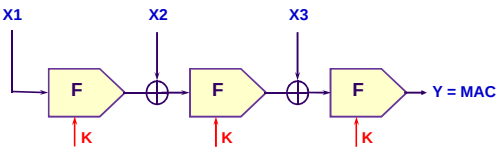
intégrité (mode f9 de KASUMI)



authentification de messages (rappel)

mode CBC - MAC

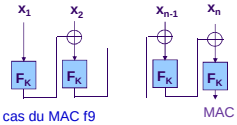
MAC = message authentication code



- seulement adapté à des messages de longueur fixe
- attaque "par collisions"
  la connaissance d'environ $2^{n/2}$ MACs permet d'en forger un nouveau

sécurité du mode f9

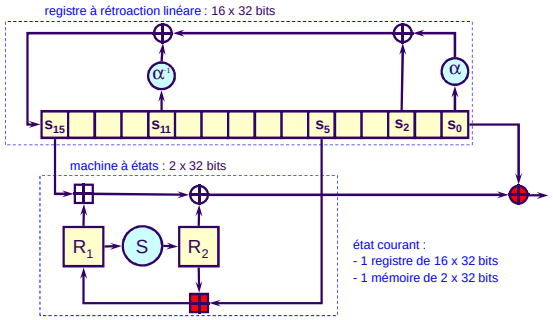
- objectifs
  - pas d'attaque réaliste de complexité << 2^{128}
  - si possible pas d'attaque permettant de forger le MAC d'un nouveau message à partir des valeurs MAC de 2^{32} messages
- cas d'un MAC CBC
  - la donnée des MAC de 2^{32} messages permet de prédire de nouveaux MAC



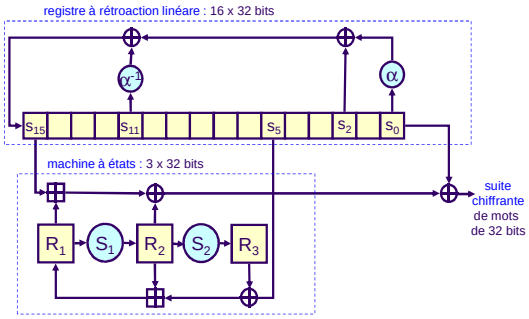
$f_K(x_1|\ldots|x_n) = f_K(x'_1|\ldots|x'_n)$
$\Rightarrow \forall\, \delta\ f_K(x_1|\ldots|x_n \oplus \delta) = f_K(x'1|\ldots|x'_n \oplus \delta)$

- cas du MAC f9
  - la meilleure attaque connue nécessite de connaître le MAC de 2^{48} messages pour forger de nouvelles valeurs de MAC [Knudsen-Mitchell]

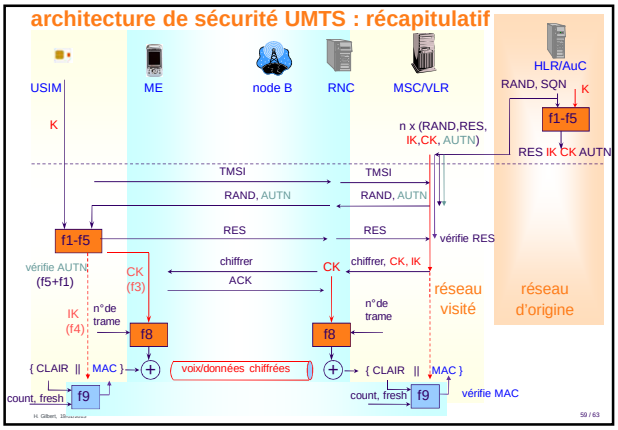
SNOW 2.0 (Université de Lund)



SNOW 3G (algorithme à flot dérivé de SNOW 2.0)



architecture de sécurité UMTS : récapitulatif



limites de la sécurité UMTS

- interfonctionnement GSM-UMTS
  - en particulier utilisation de cartes SIM 2G dans les réseaux 3G
    - CK et IK sont dérivées de la clé Kc → longueur de clé effective ≤ 64 bits
    - situation intermédiaire entre la sécurité GSM et la sécurité UMTS
- le chiffrement reste à l'initiative du réseau, qui peut décider de rester en clair
  - cependant, le réseau doit authentifier l'ordre éventuel de rester en clair (donc être reconnu de l'opérateur d'origine)
  - les attaques par fausse station de base précédentes sont inopérantes
- la séparation cryptographique n'est pas complète
  - conséquences nettement moindres que dans GSM :
    - pas d'attaques connues contre KASUMI et SNOW 3G
    - message "security mode command" obligatoire et authentifié

évolution d'UMTS : LTE / EPS

- LTE / EPC
  - EPS = evolved packet system
  - LTE = long term evolution evolved packet core)
- sous système radio

  nouvelles techniques d'accès multiple / modulation / codage
  - NodeB → eNB interconnectés, directement reliés au réseau cœur
- réseau cœur tout IP
  - MSC / SGSN → S-GW (serving gateway)
  - VLR → MME (mobility management equipment)
  - HLR → HSS (home subscriber server)

USIM

ME 

eNB 

S-GW/MME 

HSS 

LTE / EPS : architecture de sécurité (esquisse)

- SAE (system architecture evolution)
  - IK et CK servent de point de départ à la dérivation de 5 types de clés de session
    - pour la gestion de la mobilité ME-MME : chiffrement + intégrité
    - pour la gestion des ressources radio ME-eNB : chiffrement + intégrité
    - pour le trafic ME-eNB : chiffrement (s'arrête à l'eNB contrairement à l'UMTS)
- algorithmes de chiffrement et d'intégrité partiellement renouvelés
  - EPS encryption / integrity algorithms (EEA1 / EIA1) : fondés sur SNOW 3G
  - EPS encryption / integrity algorithms (EEA2 / EIA2) : fondés sur AES
  - EPS encryption / integrity algorithms (EEA3 / EIA3) : fondés sur ZUC

  (algorithmes chinois en cours d'adoption par le 3GPP)

  la séparation cryptographique entre les algorithmes est renforcée

conclusions

- sécurité de l'accès radio GSM, UMTS, EPS
  - érosion de la confidentialité des communications GSM
  - peu d'attaques actives constatées à ce jour (mais diminution du coût de telles attaques)
  - pas de vulnérabilité connue aussi grave que p.ex. celle des anciens systèmes WiFi
- évolutions en cours et impacts sur la sécurité (autres aspects)
  - multiplication des applications téléchargeables → risques accrus de "malware"
    - contre-mesures : vérification / certification de code + signature + détection de malware
  - software radio + protocoles open source → risques accrus d'attaques par déni de service
    - depuis des mobiles ou des fausses stations isolés ou coordonnés
    - contre-mesures : régulation de charge, détection d'intrusion et réaction automatique
  - infrastructures IP plus ouvertes → risques accrus d'attaques depuis le réseau fixe
    - la protection de la signalisation devient indispensable (tunnels IPSec, etc.)