Sécurité des communications en Multicast

Applications pour les liens satellites

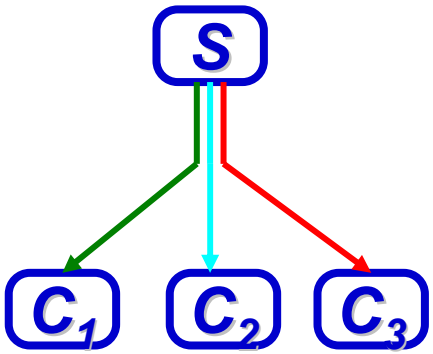
Melek Önen & Refik Molva

Institut EURECOM

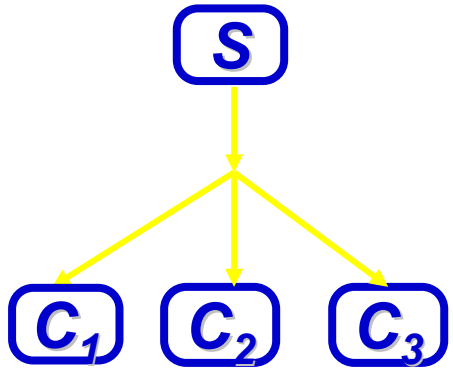
Décembre 2002

Définitions et besoins (1/2)

- Unicast : 1 → 1



- Multicast : 1 → N



- Télévision à péage
- Flux audio de haute qualité
- Mise à jour de logiciels
- Distribution de cotations boursieres

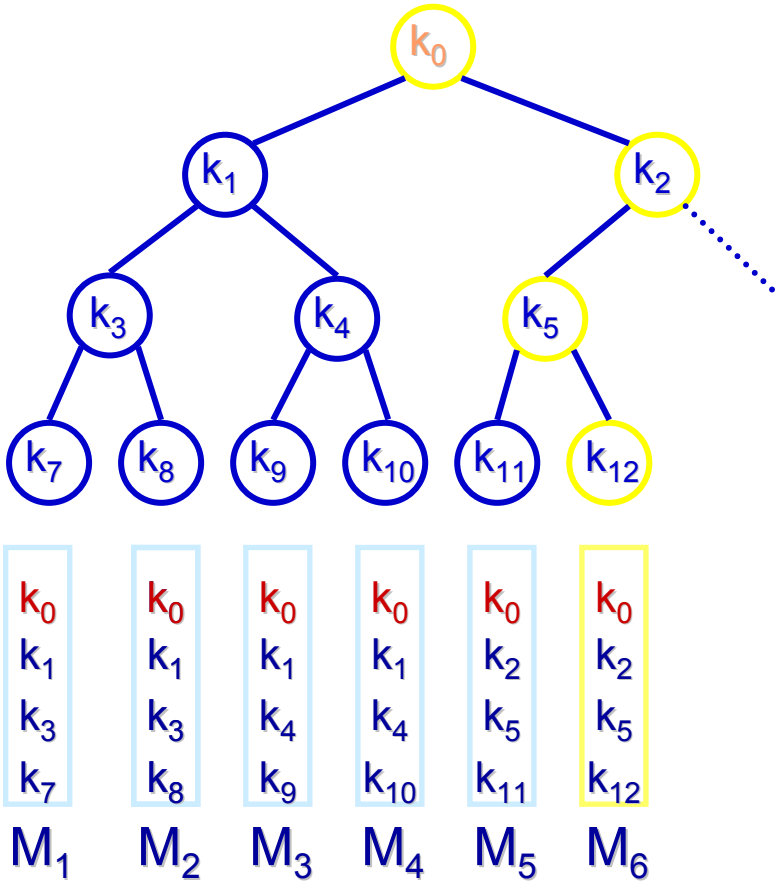
Définitions et besoins (2/2)

- Confidentialité multicast des données
  - Distribution des clefs;
  - Chiffrement.
- Authentification multicast :
  - Authentification du groupe;
  - Authentification de la source.

Confidentialité et Gestion des clefs

- Les besoins
  - Gestion d'un groupe dynamique
    - Contrôle d'accès : distribution des clefs;
    - Secret antérieur et postérieur.
  - Echelonnabilité
    - Impact minimal d'un secret divulgué : endiguement
    - Utilisation de noeuds intermédiaires : degré de confiance
- Les algorithmes :
  - Définition d'une clef pour l'ensemble du groupe
  - Répartition des membres en sous-groupes (1 clef par sous-groupe)

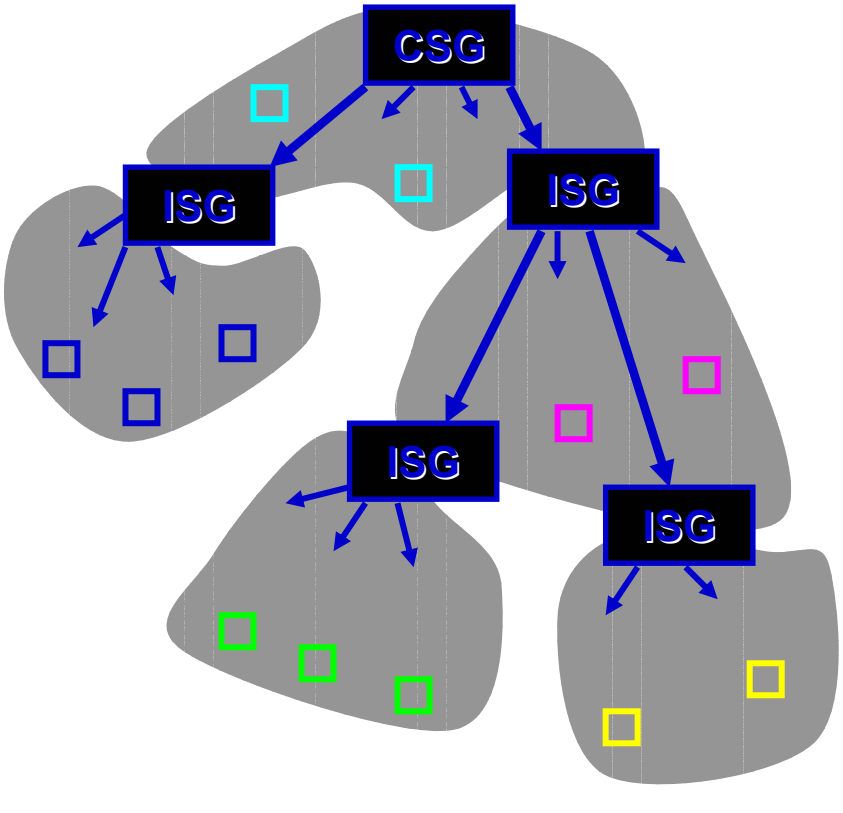
Les arbres de clefs hiérarchiques



- Avantages :
  - nombre de chiffrement en ordre logarithmique;
  - pas d'intermédiaire

- Inconvénients :
  - endiguement;
  - problème de robustesse

Les arbres de rechiffrement : Iolus

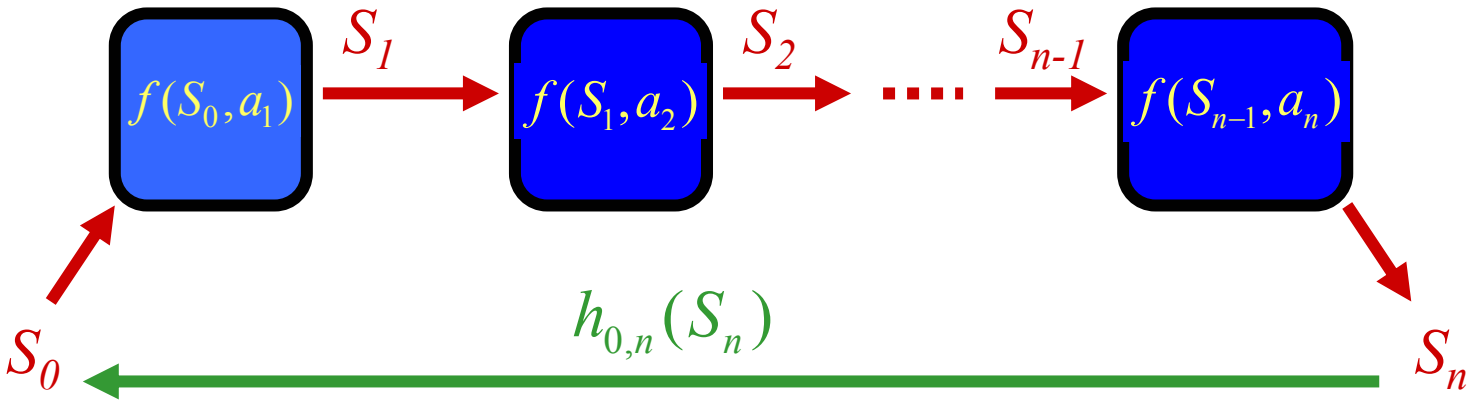


•CSG : Contrôleur de sécurité de groupe
⇒ définit le groupe et les ISG;
•ISG : Intermédiaire de sécurité de grou
⇒ déchiffre un paquet qu'il reçoit
⇒ rechiffre pour son groupe fils

• Avantages :
- échelonnabilité
- clef d'accès locale : endiguement
• Inconvénient :
- confiance aux noeuds intermédiaire

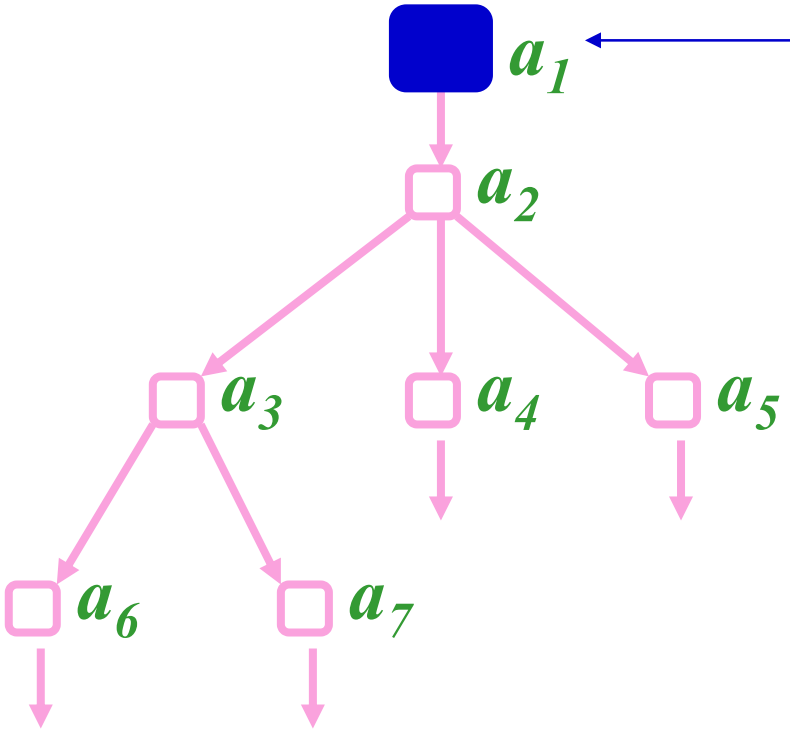
Suite paramétrée de chiffrement

- Rôle actif des noeuds intermédiaires
- Suites réversibles



- Technique symmétrique et/ou asymmétrique

Description de la technique

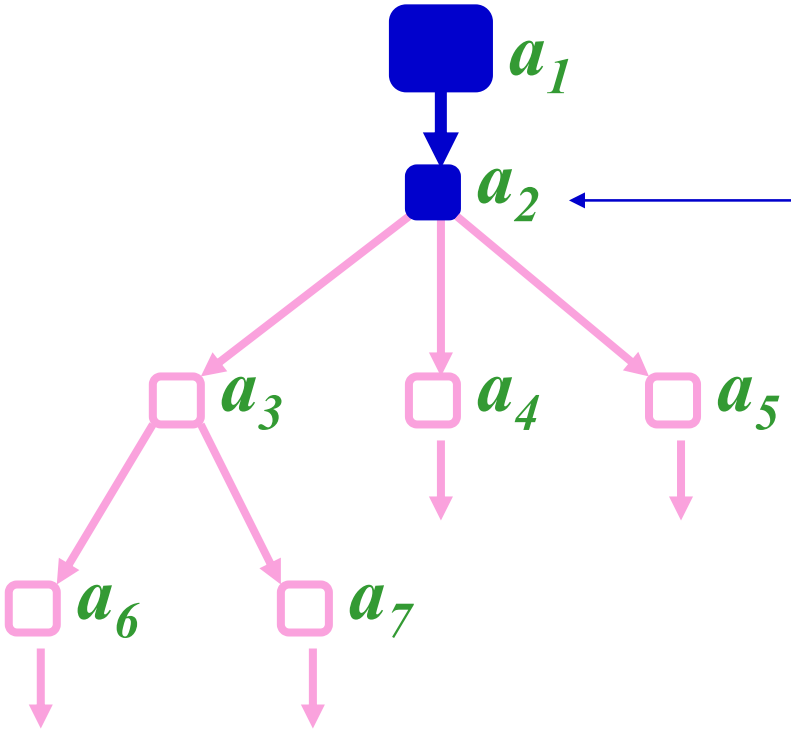


La Source envoie :

$$S_1 = (S_0)^{a_1} \bmod p$$

$$T = M \oplus S_0$$

Description de la technique

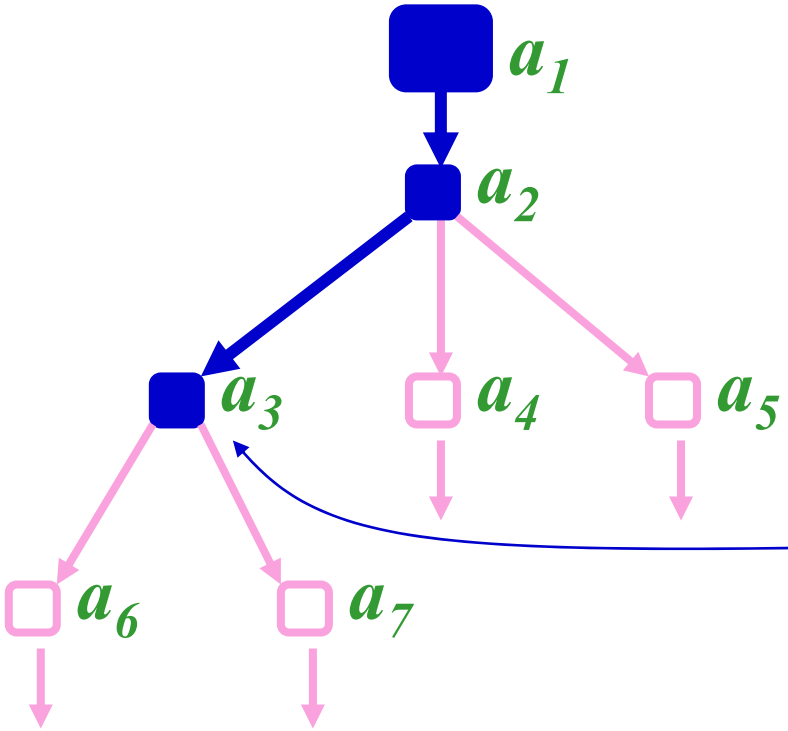


Le noeud envoie :

$$S_2 = (S_0)^{a_1 a_2} \bmod p$$

$$T = M \oplus S_0$$

Description de la technique

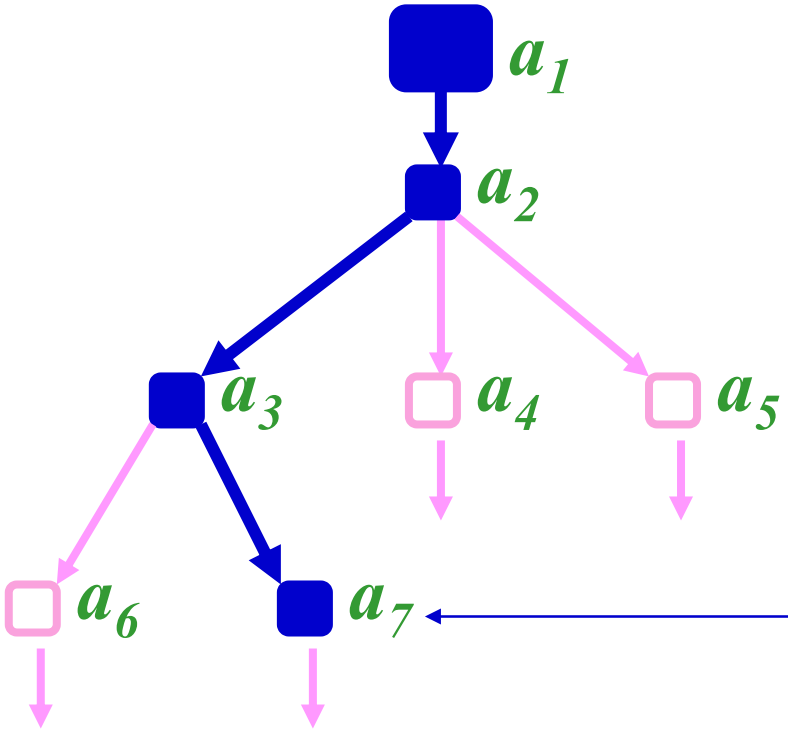


Le noeud envoie :

$$S_3 = (S_0)^{a_1 a_2 a_3} \bmod p$$

$$T = M \oplus S_0$$

Description de la technique

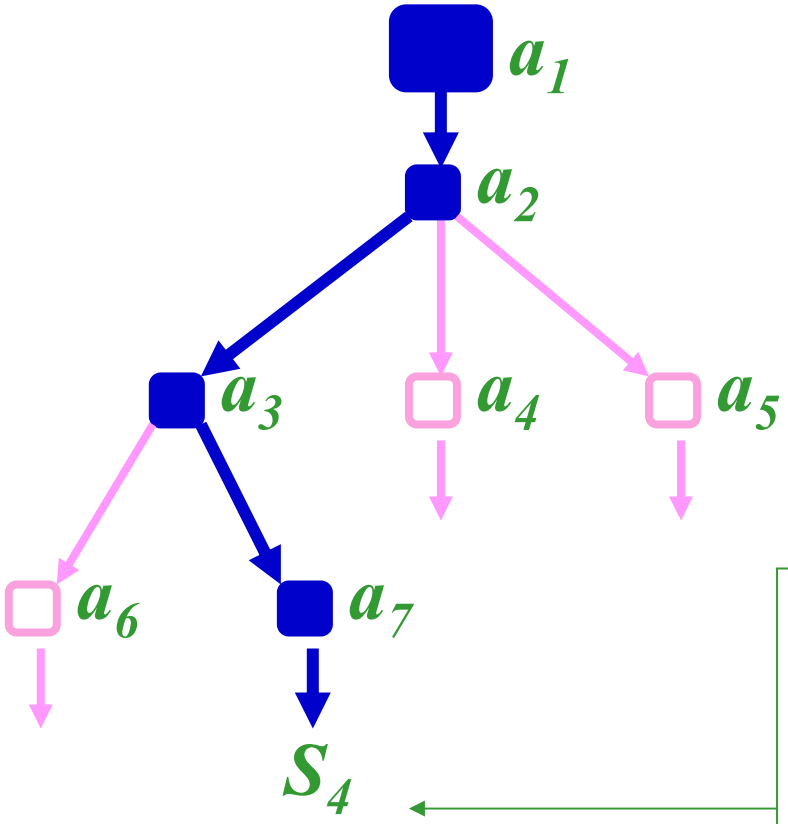


Le noeud envoie :

$$S_4 = (S_0)^{a_1 a_2 a_3 a_7} \bmod p$$

$$T = M \oplus S_0$$

Description de la technique



$$S_1 = (S_0)^{a_1} \bmod p$$

$$T = M \oplus S_0$$

Les membres locaux :

$$S_0 = (S_4)^{\frac{1}{a_1 \cdot a_2 \cdot a_3 \cdot a_7}} \bmod p$$

Propriétés de cette technique

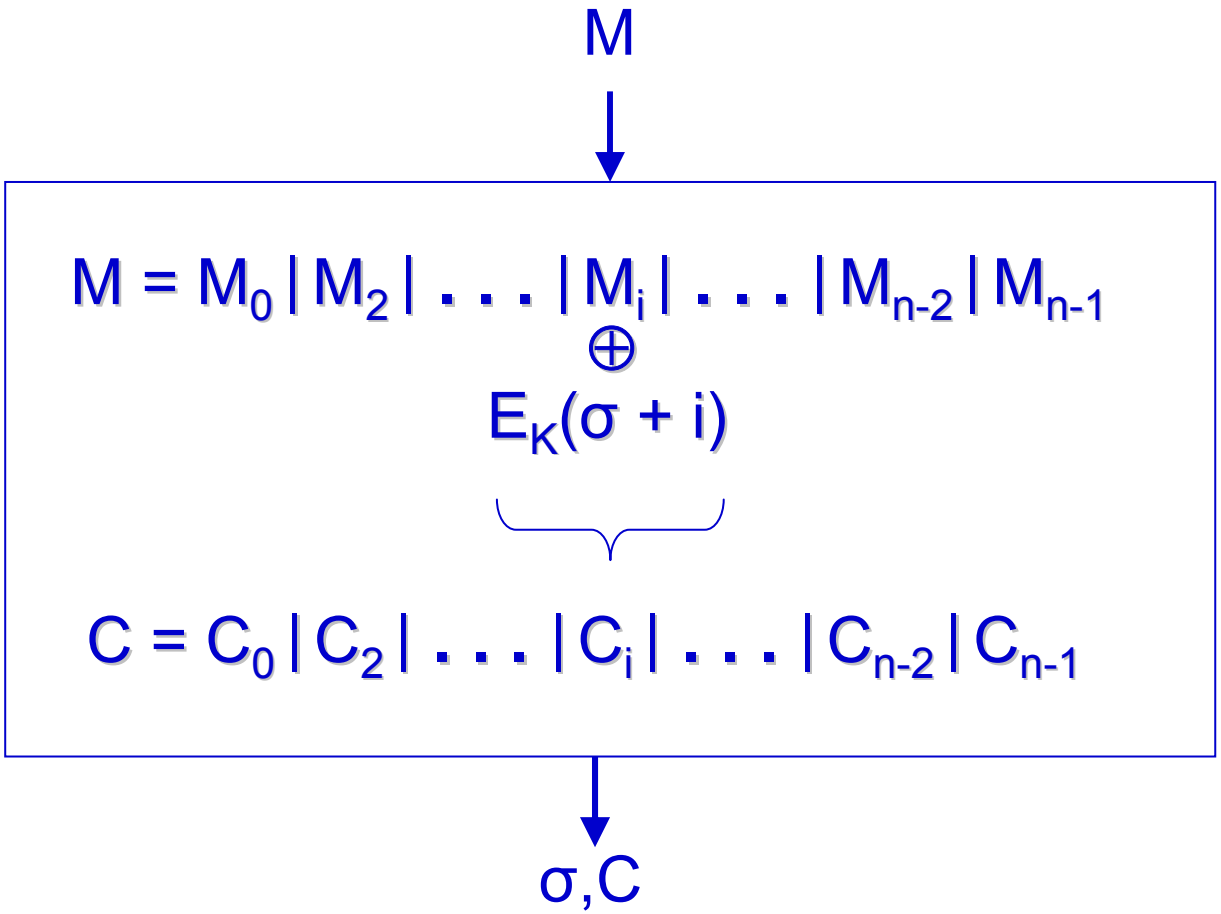
- Pas de confiance aux nœuds intermédiaires
  - Aucun accès aux données en clair;
  - Transformations transparentes .
- Endiguement :
  - Clefs d'accès différentes selon le lieu du récepteur;
  - Impact de dynamicité du groupe local au sous-groupe.
- Coût :
  - Pas efficace pour des chiffrement de paquets abondants
  - Applicable pour des schémas de distribution de clefs.

Chiffrement multi-couches

- But : Combinaisons des avantages des deux schémas utilisant des arbres de rechiffrement pour un chiffrement plus efficace avec les avantages d'endiguement et d'échelonnabilité.

- Solution: Utilisation de l'opération XOR (counter mode)
  - Chiffrement en plusieurs couches du coté de la source et des récepteurs
  - Les noeuds intermédiaires :
    - Une opération de déchiffrement symmétrique
    - Une opération de chiffrement symmétrique

Counter Mode (CTRM) Encryption



- [Bellare et al] Security Equivalent to PRF E

CTRM multi-couches

$$M_i = 01010101101111010111110 1\ldots$$
$$\oplus$$
$$P_{K1}(i) = E_{K1}(\sigma_1, i) = 10100100100100100010111 11\ldots$$
$$\oplus$$
$$P_{K2}(i) = E_{K2}(\sigma_2, i) = 10100001000101110000000 1\ldots$$
$$\oplus$$
$$P_{K3}(i) = E_{K3}(\sigma_3, i) = 10100001000101110000000 1\ldots$$
$$C_i = 11110001001011110101001 0\ldots$$

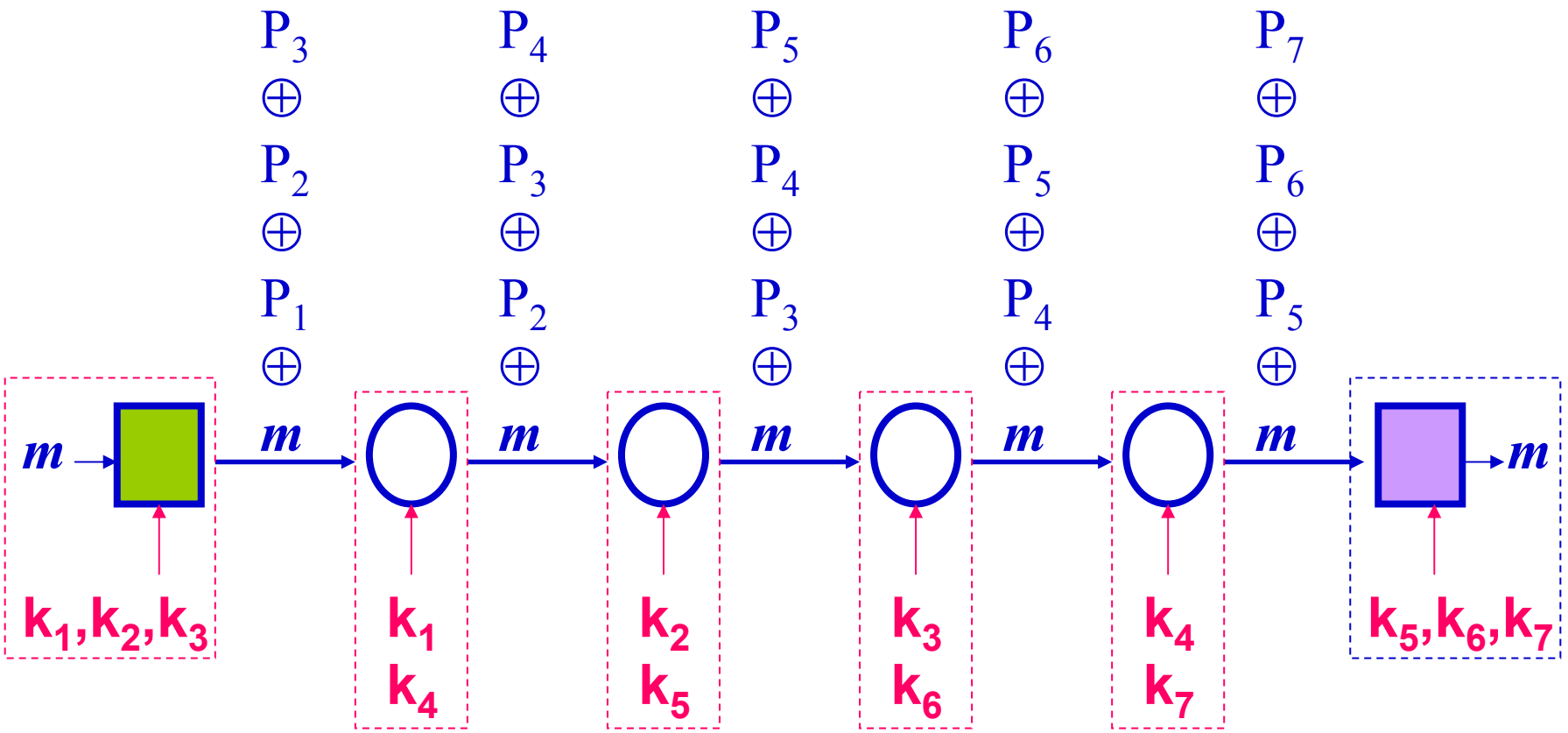
$C = M \oplus P(k_1) \oplus P(k_2) \oplus P(k_3)$

$C' = M \oplus P(k_1) \oplus P(k_4) \oplus P(k_3)$

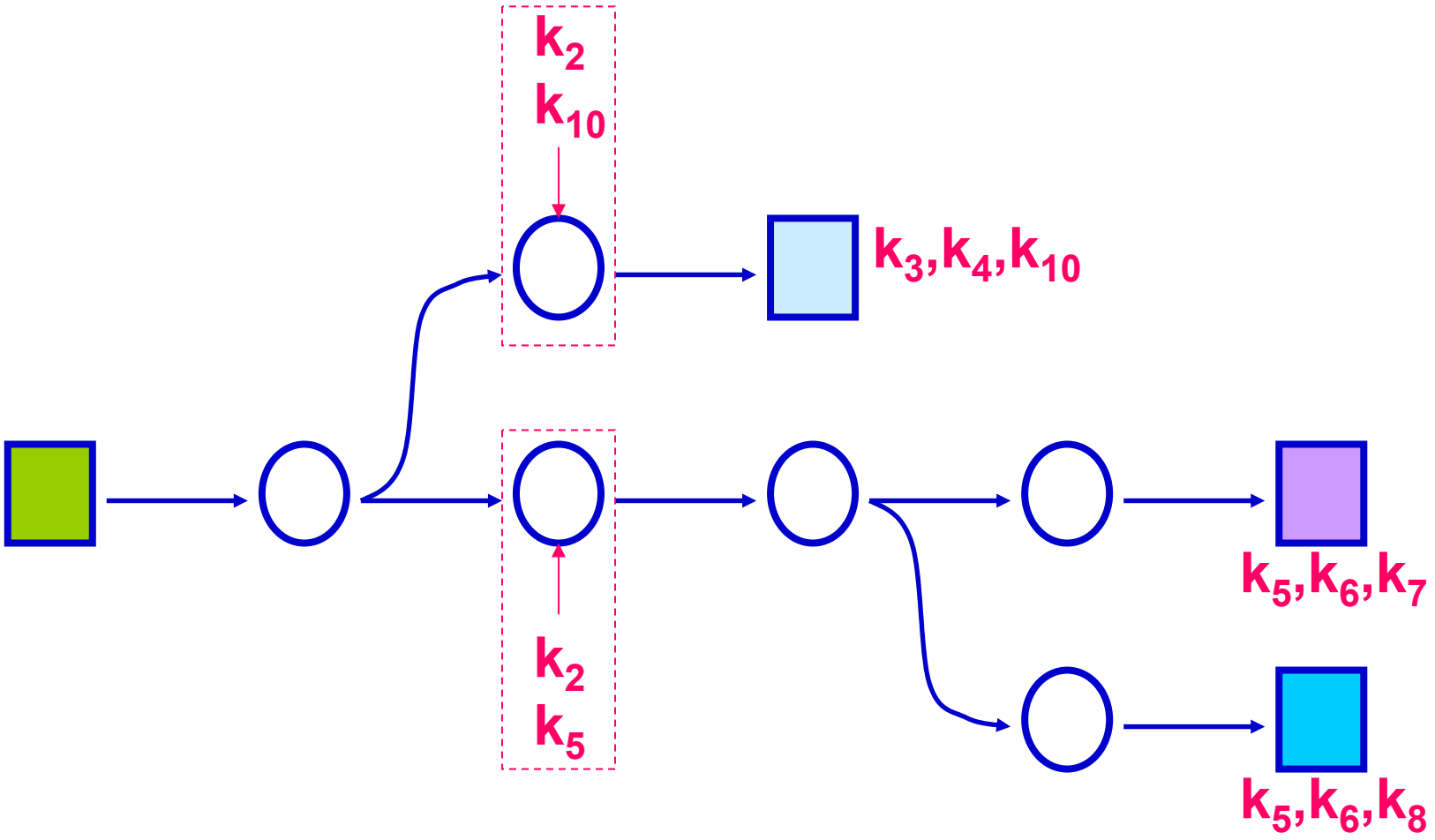
$C \oplus P(k_2) \oplus P(k_4)$

intermédiaire

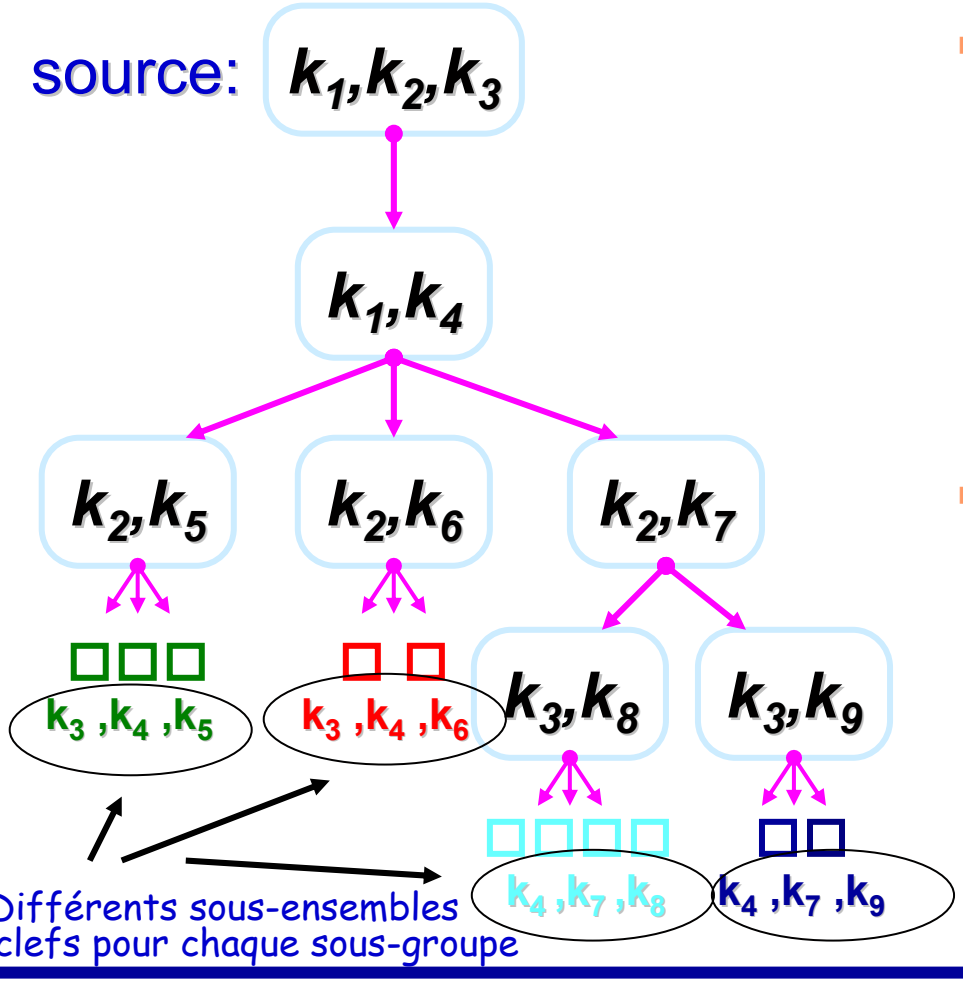
Modèle pour un lien



Modèle pour un groupe

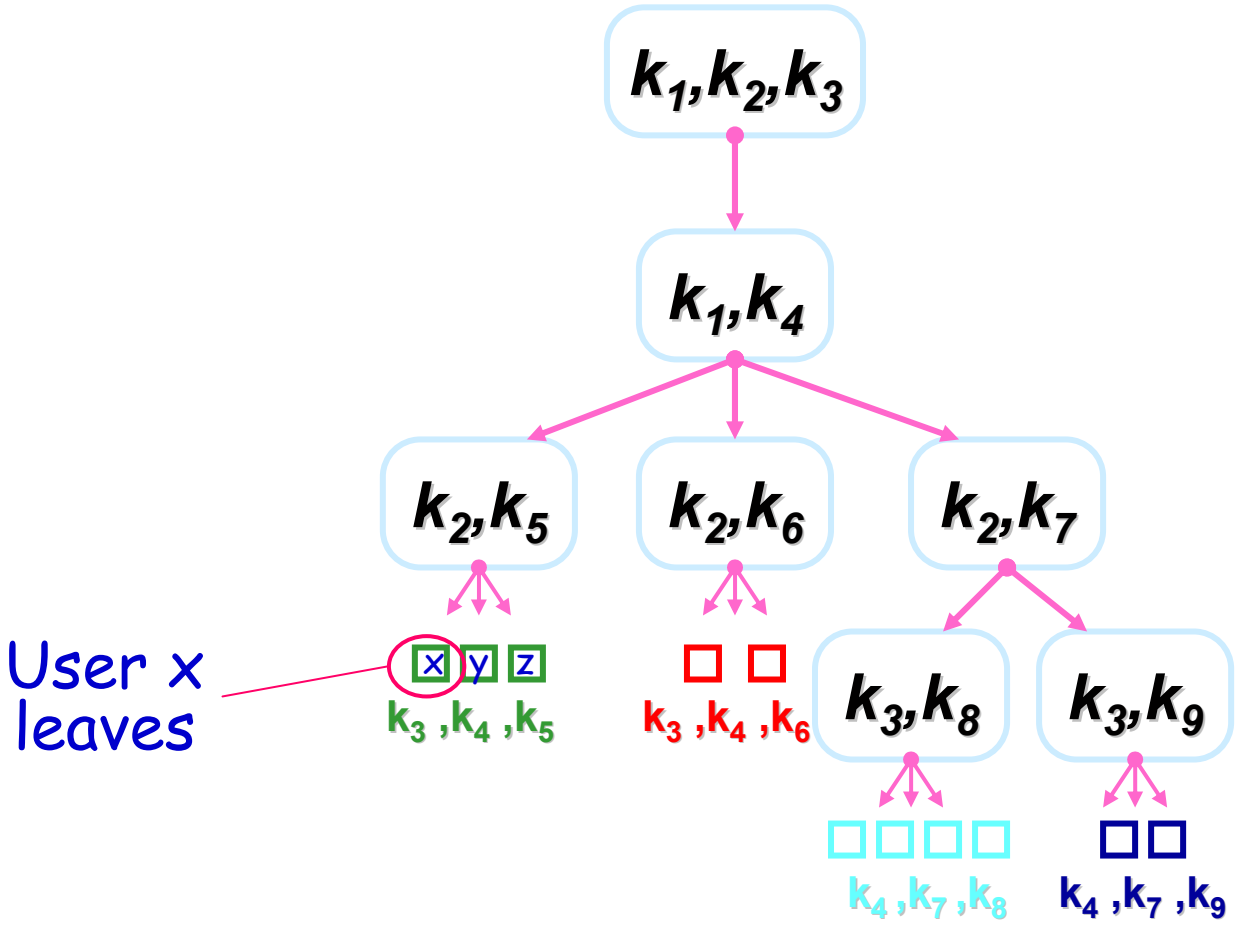


Arbres de communication en L-couches

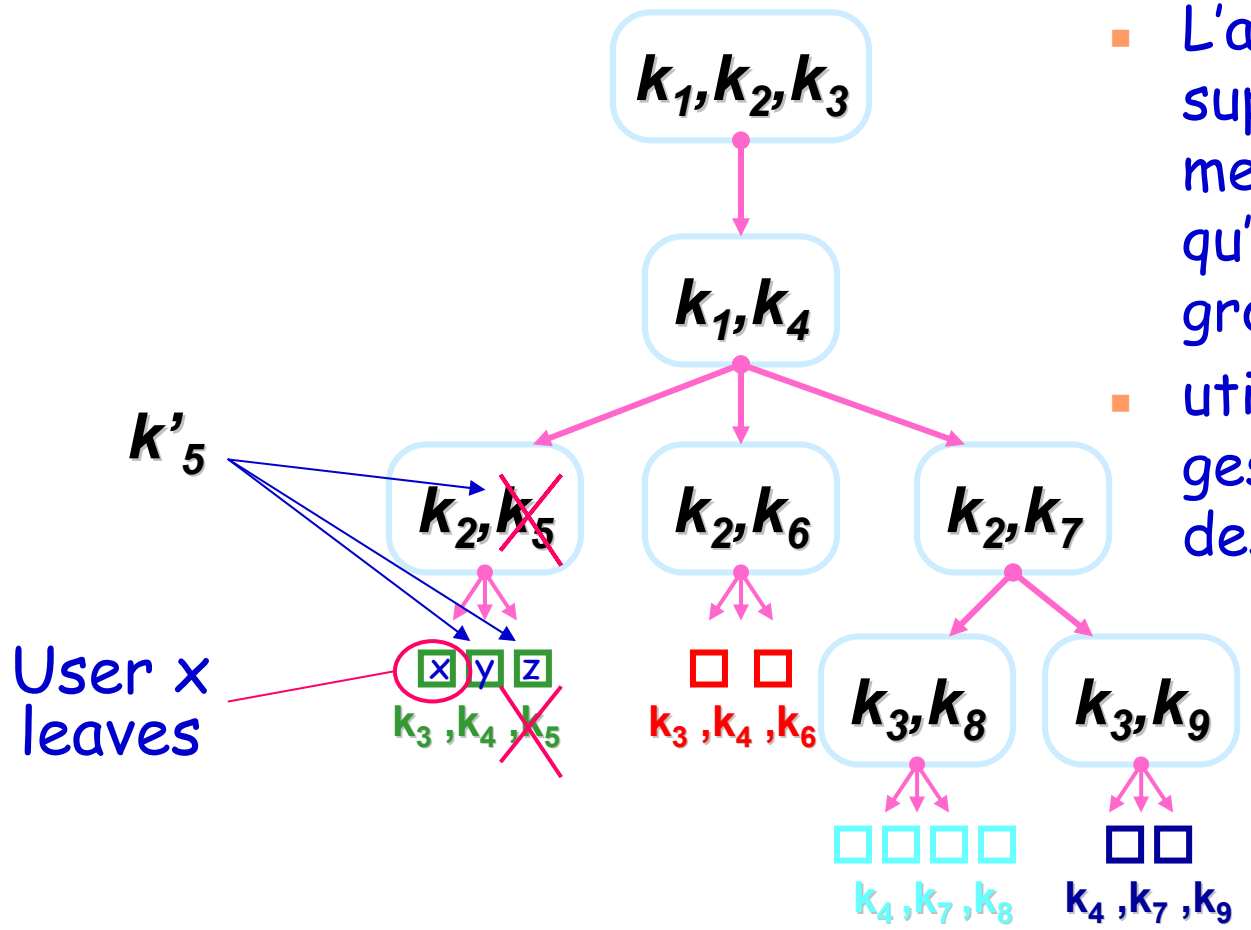


- Coût.
  - Source: L opérations.
  - Récepteur: L opérations.
  - Intermédiaires: 2 opérations.
- Avantages:
  - Utilisable pour le contenu.
  - Confiance limitée aux intermédiaires.

Gestion de la dynamicité du groupe



Gestion de la dynamicité du groupe



- L'adhésion et la suppression d'un membre n'affecte qu'une partie du groupe
- utilisable pour une gestion distribuée des membres

Conclusion

- Deux schémas pour la confidentialité
  - Définition d'une clef de groupe globale et réduir le coût de la distribution (ex arbres de clefs)
  - Définition de clefs de sous-goupes selon leur localité : utilisation de nœuds intermédiaires
    - Confiance totale aux nœuds intermédiaires : Iolus
    - Pas de confiance : suite paramétrée de chiffrement
  - Le chiffrement multi-couches : une solution unique offrant :
    - Echelonnabilité
    - L'endiguement
    - Le chiffrement de données massives

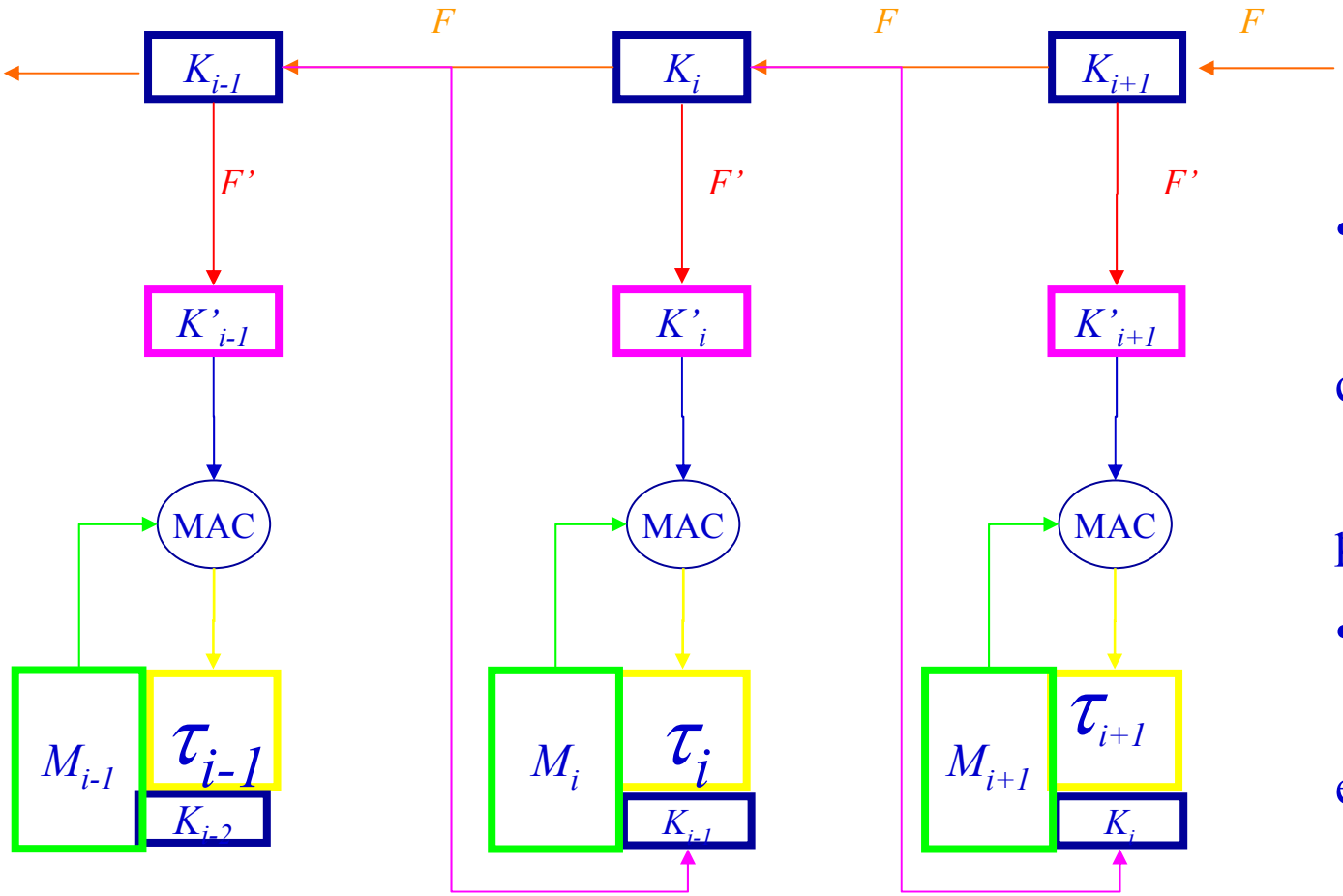
Authentification multicast

- Une suite de paquets à authentifier individuellement.
  - Nécessite une authentification peu coûteuse en espace et en calcul par paquet.
  - Implique l'utilisation de techniques cryptographiques symétriques.

- Une situation asymétrique :
  - 1 générateur de contenu et *n* vérificateurs
  - Implique l'utilisation de techniques cryptographiques asymétriques chères et coûteuses en espace.

→ Un dilemme.

Chaînage temporel : TESLA



•Avantages :

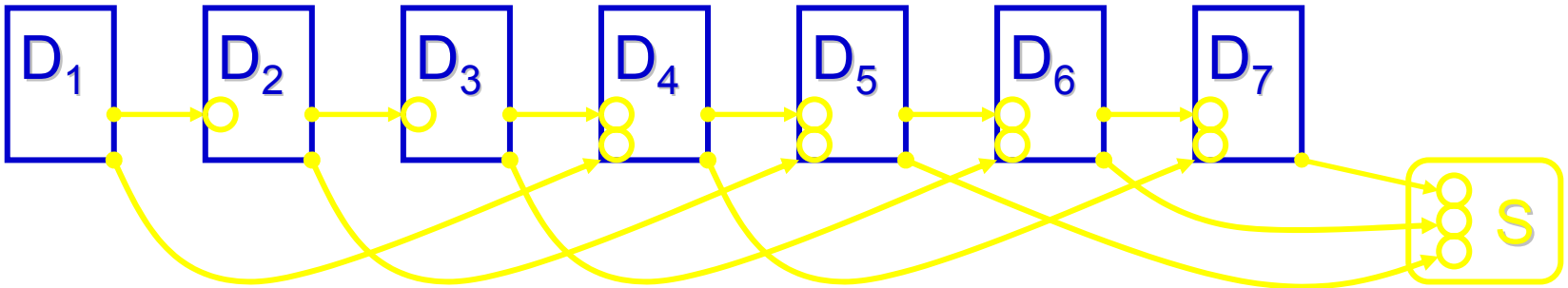
- opérations non coûteuses

- tolérance aux pertes

• Inconvénient :

- synchronisation entre S et C

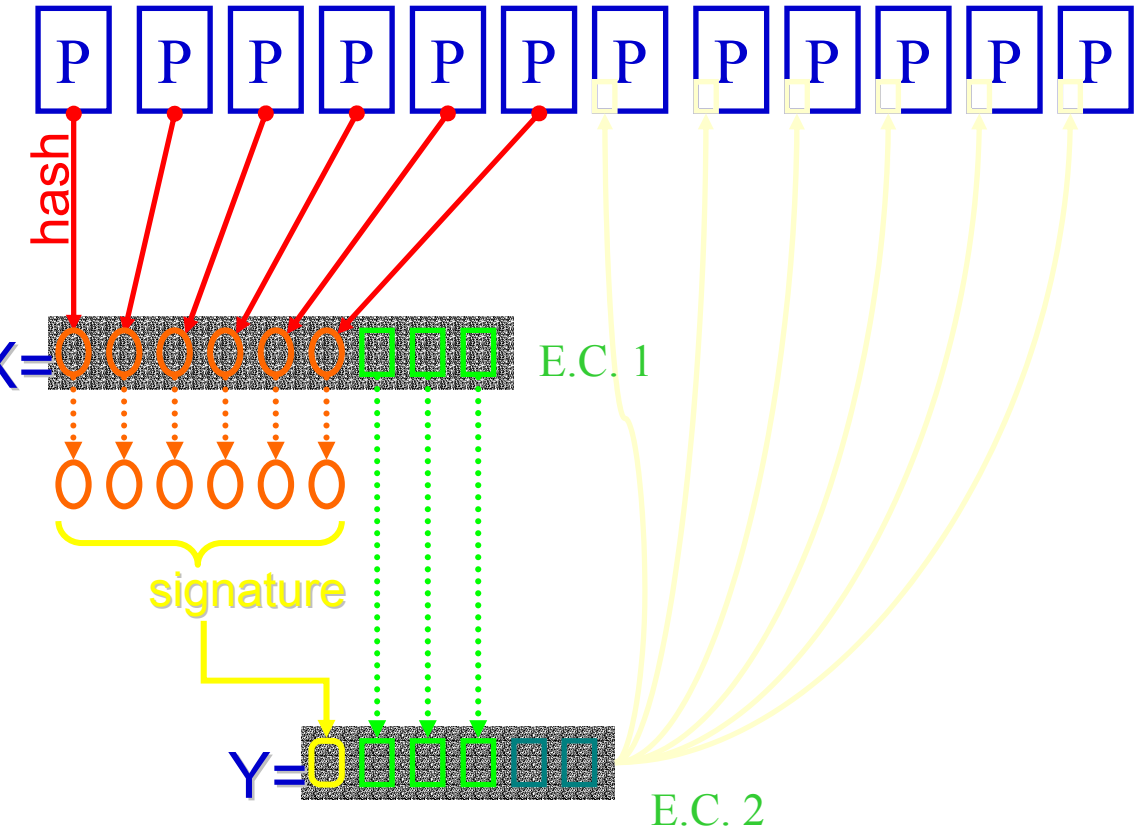
Chaînages par hachages :EMMS



•Avantages :
- opérations pas coûteuses et contrôlées;
- tolérance aux pertes;

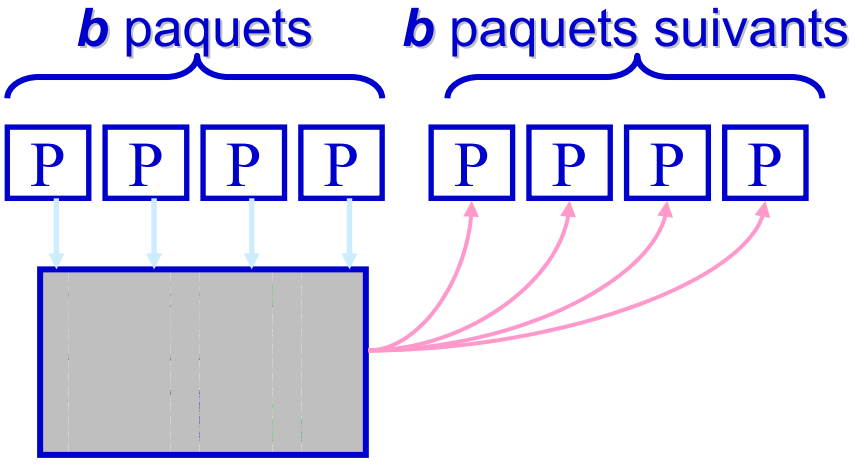
• Inconvénients :
- “comment calculer la taille *b* d’un bloc ?”

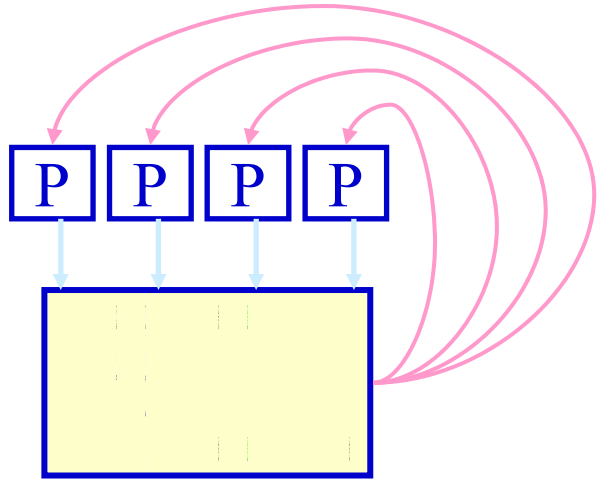
Utilisation des FECs

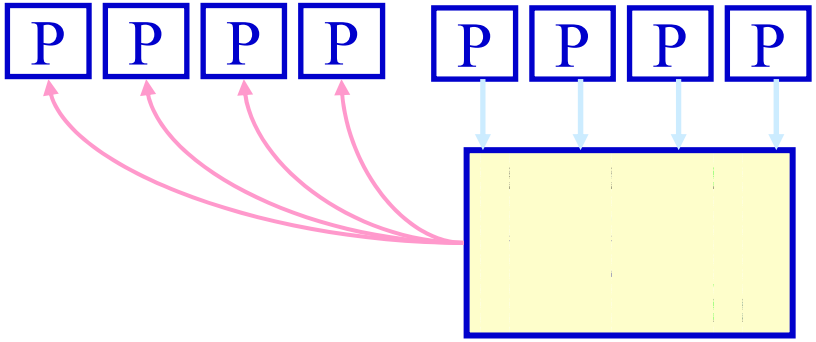


- Avantages :
  - réduction du coût de la signature
  - tolérance aux pertes
- Inconvénients :
  - calcul des codes reconstructeurs

3 modes







Influence:

- Tampon serveur
- Délai d'authentification

Conclusion

- Authentification:
  - Chaînage des MACs de messages au cours du temps
    - Opérations non coûteuses mais synchronisation indispensable
  - Chaînage des hachages
    - Opérations non coûteuses et indépendance temporelle
    - Signatures fréquentes
  - Utilisation des codes correcteurs d'erreurs
    - Réduction du coût de la signature
    - Coût en terme de calcul des FECs
    - Application aux distributions de données en temps réel

Références

- "Secure group communications using keygraphs", Wong et al, 1998.
- "Iolus : A framework for scalable secure multicasting", Mittra, 1997.
- "Scalable multicast security with dynamic recipient groups", Molva et al, 2000
- "Multiple Layer encryption for Multicast groups", Pannetrat et al, 2002.
- "Efficient authentication and signing of multicast streams over lossy channels", Perrig et al, 2000.
- "Authenticating Real Time Packet Streams and Multicasts", Pannetrat et al,2002.

La sécurité pour les liens satellites

Eurécom & AlcatelSpace

La sécurité pour les liens satellites

- Services offerts
- Systèmes existants & futurs
- Caractéristiques des systèmes satellites et besoins en sécurité
- SATIPSec

La sécurité pour les liens satellites

- Services offerts par un système satellite
- Systèmes existants & futurs
- Caractéristiques des systèmes satellites et besoins en sécurité
- SATIPSec

Les services offerts

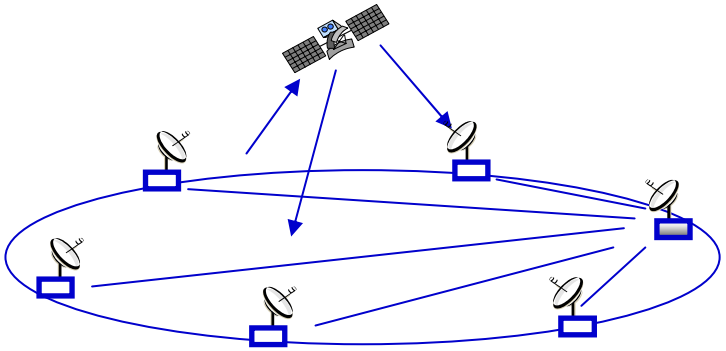
- Observation
  - Systèmes dédiés
- Diffusion
  - Broadcast TV transparent
  - Bouquets numériques
- Diffusion avec interaction faible
  - Télé-enseignement, meeting : UDLR (retour terrestre)
  - Accès Internet
- Interconnexion point à point
  - Trunck haut-débit (20 Mbit/s)
  - Vsat téléphonique (64kbit/s)

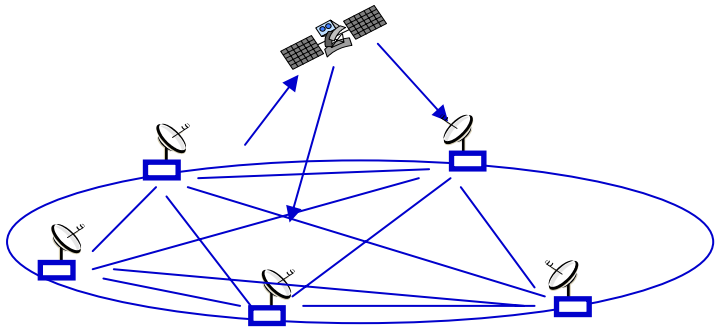
Equipements

- Equipement utilisateur
  - E1, PABX, réseau ethernet, réseau ATM, ...
- Terminal satellite (ST)
  - Interface, adaptation, couche MAC, couche Phy, antenne
- Satellite
  - Transparent (Phy), Transparent/commutation Phy, OBP (MAC)
  - Contrôle du positionnement : TMTC
- Hub
  - Concentrateur d'acces pour les terminaux
  - NCC (Network Control Center): DAMA
- Réseau

Topologie

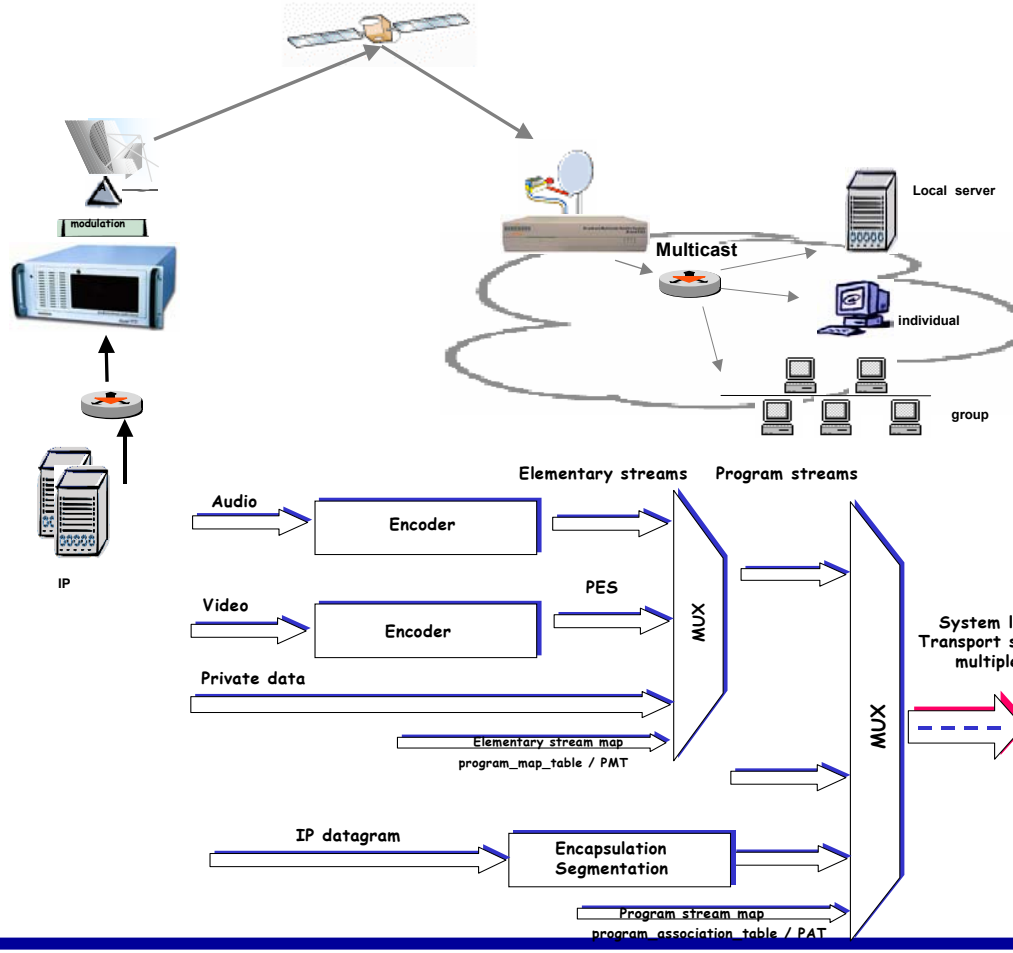
- Système Star
  - Liaison inter-ST, via le hub
- Système Mesh
  - Liaisons ST directes





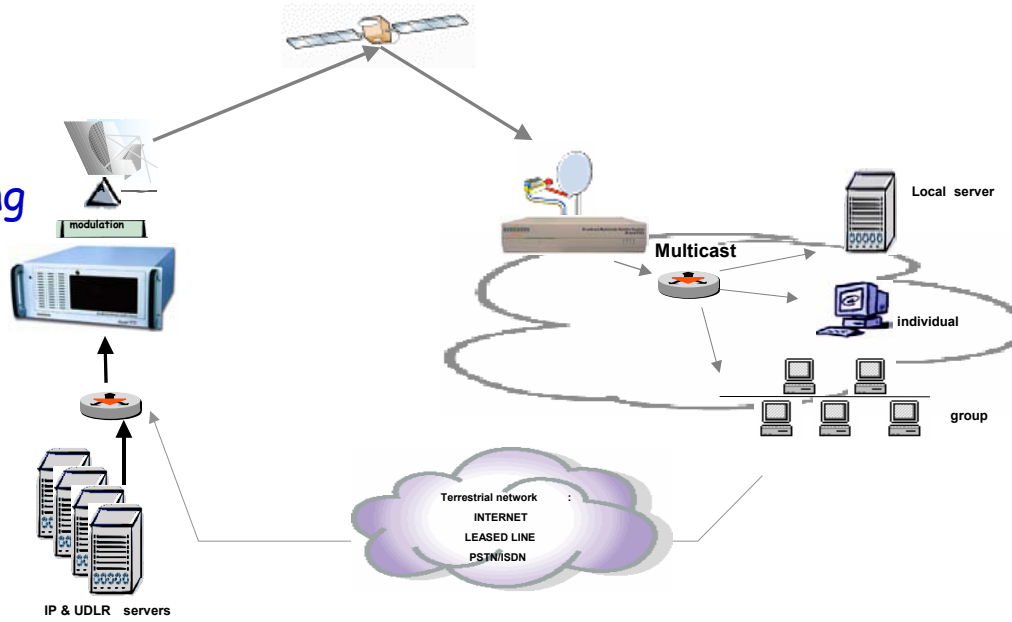
Les systèmes existants - DVB-S

- ETSI Standard
  - European Telecommunications Standards Institute
  - Digital Video Broadcasting (DVB)
  - DVB-S: Satellite
  - DVB-T: Terrestrial
  - DVB-C: Cable
  - Audio/ Video/ Programs/ Network packets/ Private data
  - Extensions for IP (Internet Protocol)



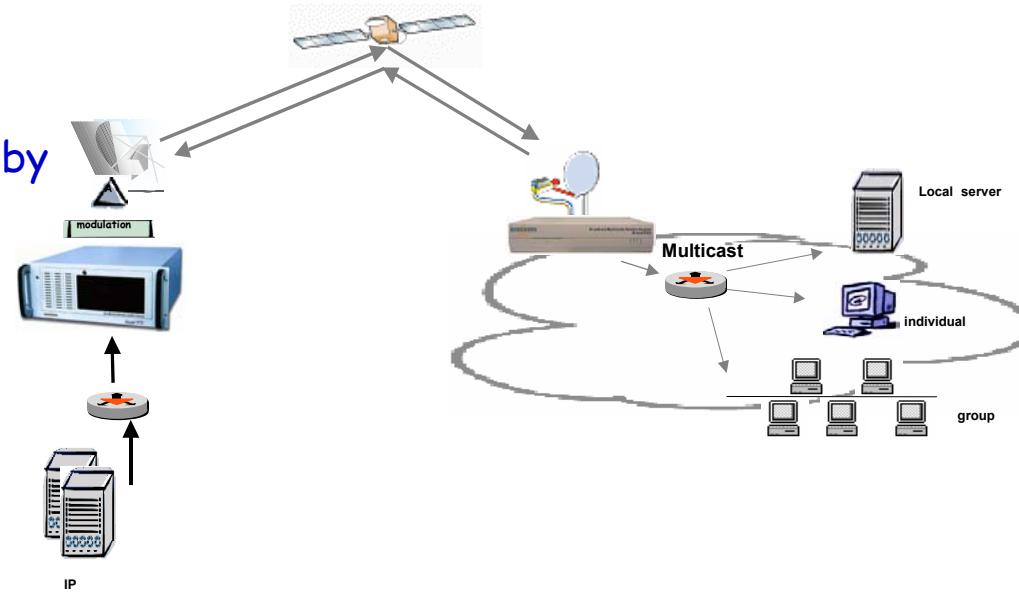
DVB-S/UDLR

- Forward
  - DVB-S link
- Return
  - Tunnel terrestre
  - UniDirectionnal Link Routing
  - IETF RFC 3077
  - IETF: Internet Enginering Task Force



DVB-S/DVB-RCS

- Forward
  - DVB-S
- Return
  - DVB-RCS: return channel by Satellite
  - IP over ATM cells
  - IP over MPEG2 frames.
  - ETSI standard



Caractéristiques des liens satellites

- Délai de transmission non négligeable
  - Satellites géostationnaires 250ms
- Capacités natives de broadcast-multicast
  - Un seul pqauet pour des milliers de récepteurs
- Couverture étendue
  - 1 spot peut recouvrir le continent européen
  - 1 station Hub gère des milliers de terminaux
- Coût du lien
  - Les liens satellites point-à-point sont beaucoup plus coûteux par rapport à ceux terrestres
  - Fiabilité de transmission indispensable

Les besoins de sécurité

- Gestion du réseau satellite
  - Contrôle et gestion des terminaux
  - Contrôle du satellite (TM-TC)

- Sécurité du plan de données
  - Niveau 3 : IPSec modifié
  - Niveau 2 : protocoles souvent dédiés
  - Niveau 1 : applications militaires

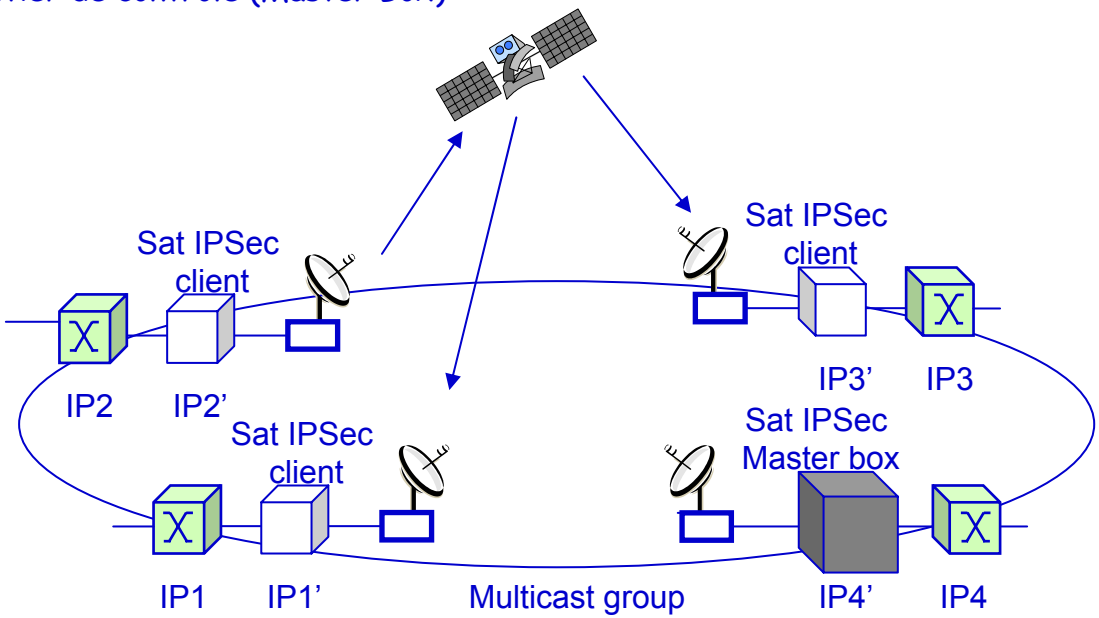
Sécurité Niveau 3 : IPSec et ses limites

- Les faiblesses du lien satellite
  - Tout le monde est à l'écoute
  - Chacun peut émettre
  - Sécurité du lien satellite est suffisante pour les opérateurs

- IPSec
  - IPSec et IKE ne sont pas fiables pour les communications multicast
  - Un très grand nombre de liens unicast devrait être créé
  - Dans le cas des réseaux terrestres, sécuriser *n* liens unicast peut être acceptable
  - Pour les réseaux satellite cela signifie une perte de la capacité native du satellite de broadcast

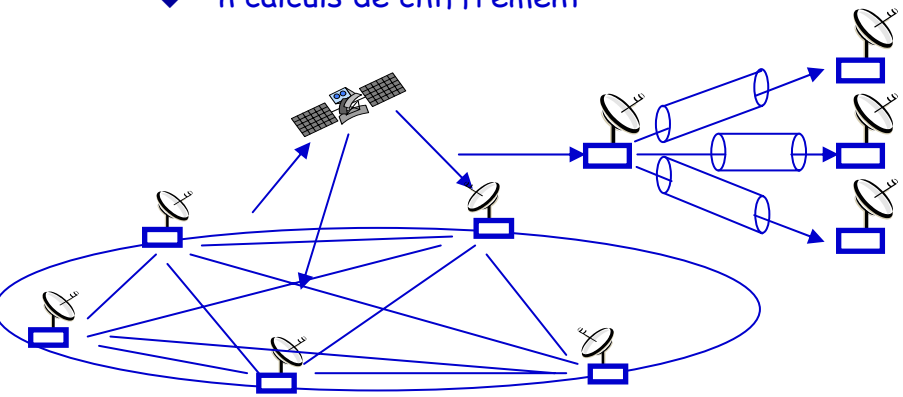
SATIPSec Architecture

- Terminal Satellite
  - Chiffrement des paquets en entrée
  - Déchiffrement des paquets en sortie
- Gestion et contrôle centralisés
  - Un boitier de contrôle (Master Box)

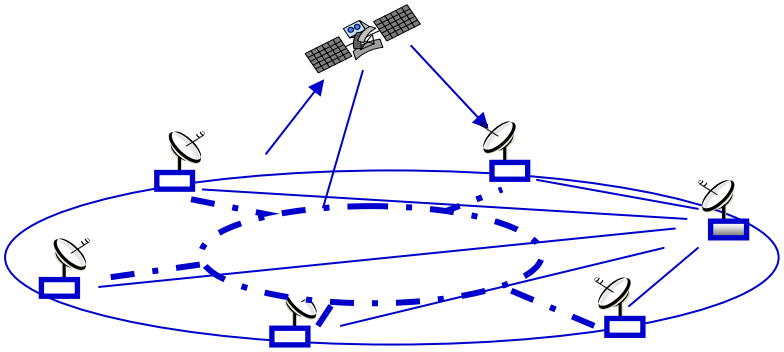


Comparaisons IPSEC - SATIPSec

- IP Sec est utilisable, mais pas optimisé pour du multicast
  - n! liaisons sécurisées
  - 1 établissement de session (10 messages minimum) par liaison
  - 1 configuration de chiffrement propre à chaque liaison
  - Duplication des paquets multicast chiffrés sur chaque liaisons
  - n calculs de chiffrement



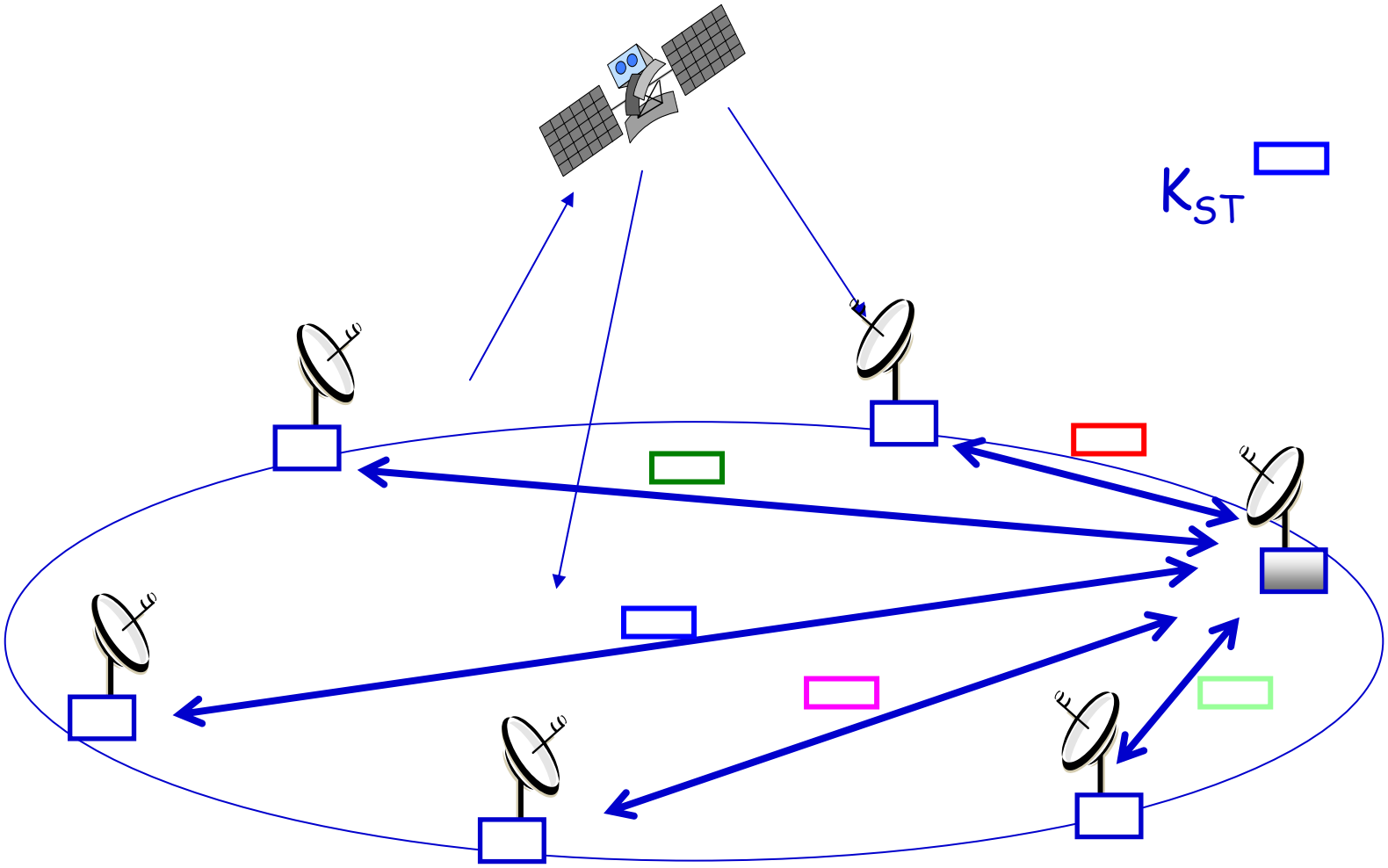
- Sat IP Sec
  - Séparation des plans de contrôle, et données
  - Une liaisons de contrôle entre chaque terminal et le serveur central
  - 1 seul établissement de session par terminal
  - 1 configuration de chiffrement des données partagé par tous les terminaux
  - un paquet **unicast** ou **multicast** chiffrés par un term est déchiffrable par tous les autres.



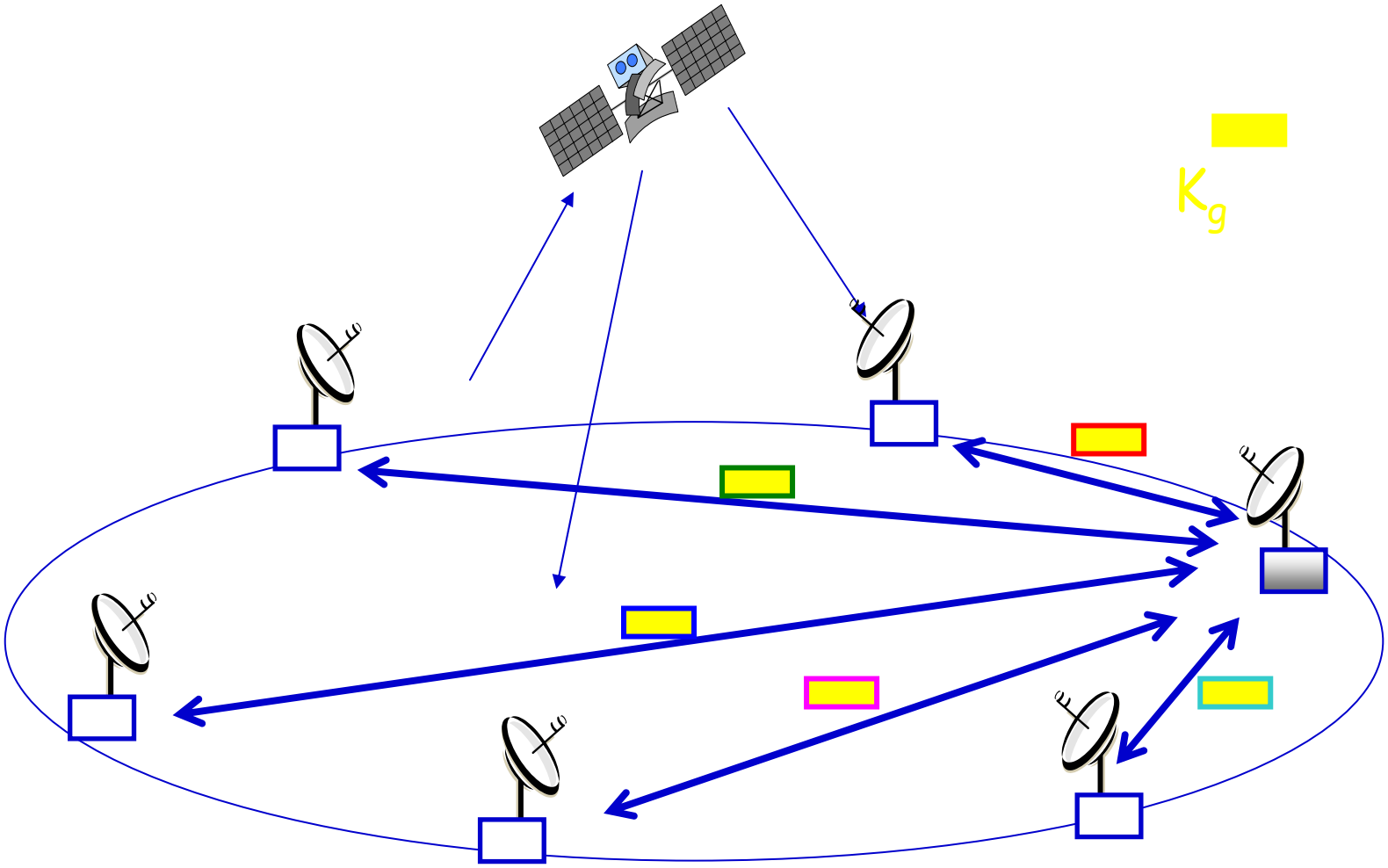
SATIPSec : Phases

- Phase 1 (Unicast) :
  - Négotiation des paramètres de sécurité (algorithmes, clefs,etc.)
  - Authentification mutuelle
  - Définition d'une clef indviduelle pour chaque ST
- Phase 2 (Unicast) :
  - Renouvellement de la clef individuelle
  - Distribution de la première clef de groupe
- Phase 3 (Multicast) :
  - Renouvellement de la clef de groupe
  - Mise à jour de la configuration du plan de données

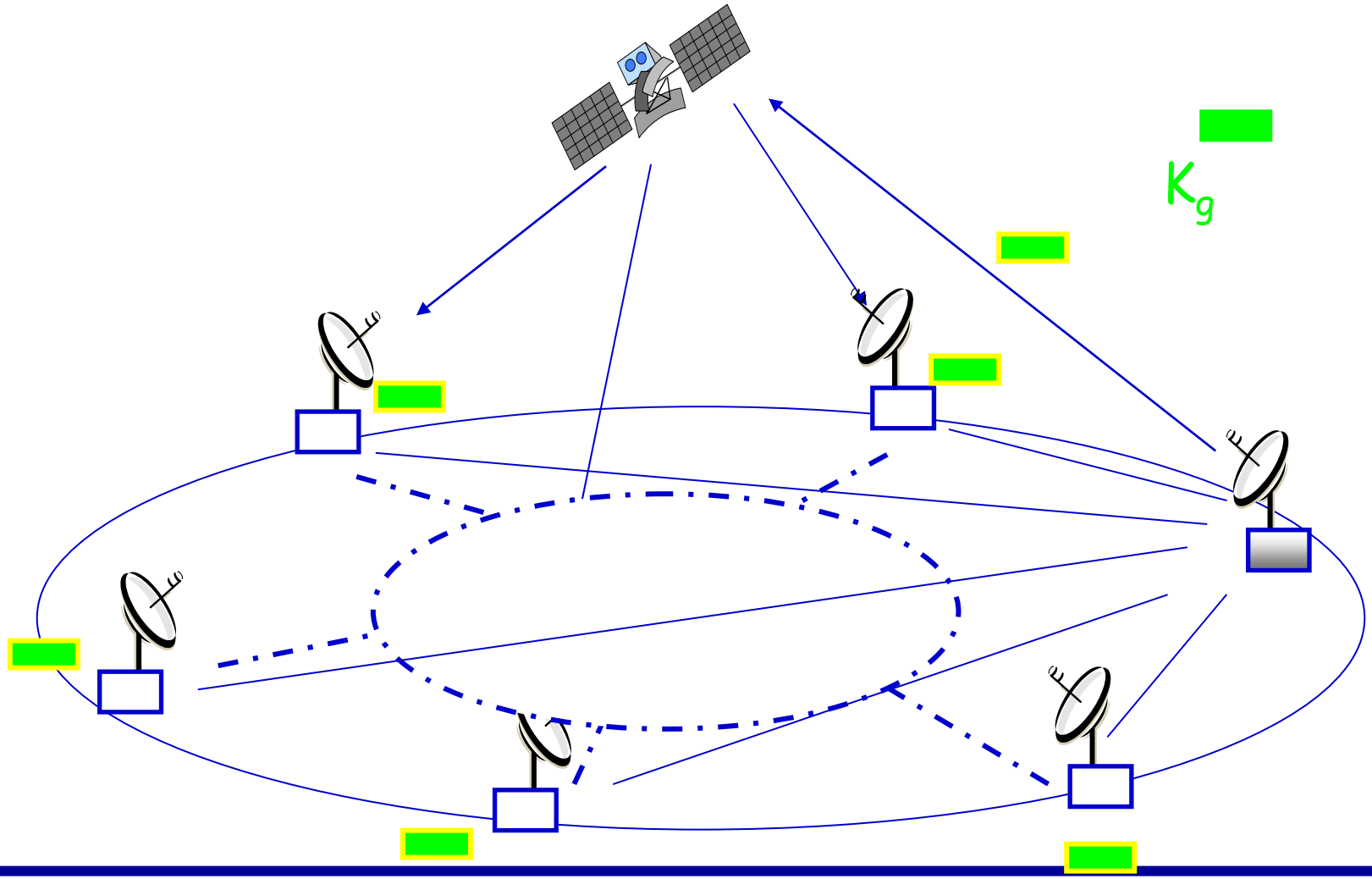
SATIPSec – Phase 1 (Unicast)



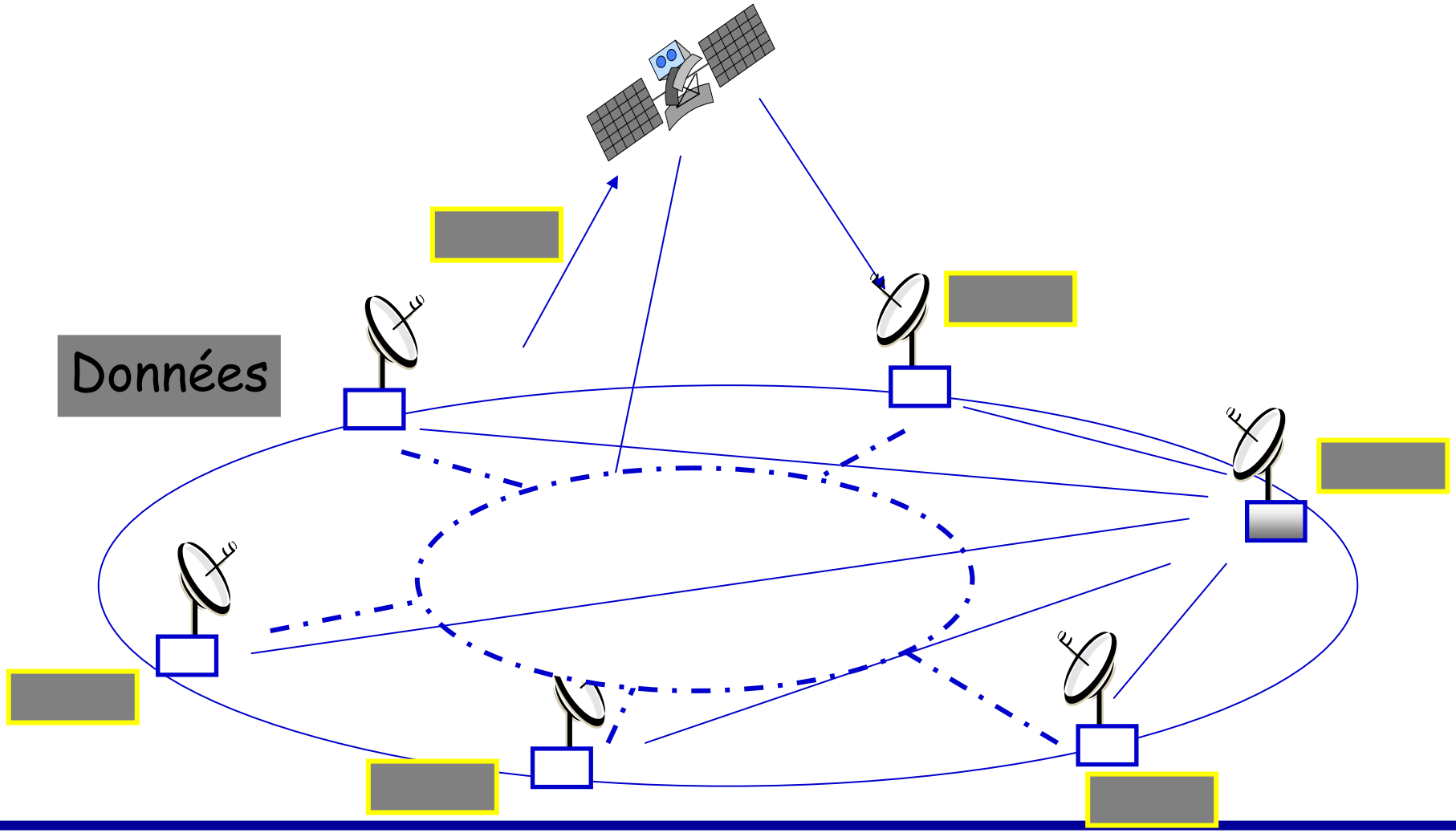
SAT IPSec -Phase 2 (Unicast)



SATIPSec : Phase 3 (Multicast)



SatIPsec : Plan de données (Multicast)



Perspectives

- Gestion de la dynamicité du groupe où le nombre des membres est très important
  - Application et comparaison des algorithmes de distribution de clefs
- Gestion de la fiabilité
  - Gestion actuelle : ACK, NACK selon la phase
  - Définir un algorithme de distribution de clefs fiable