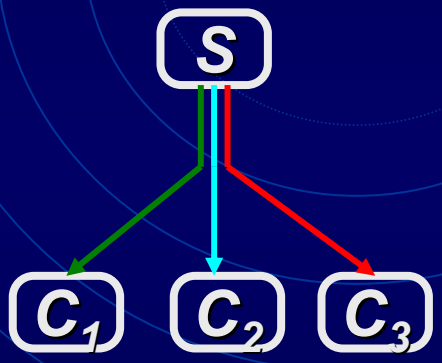
La sécurité des communications multicast

Melek ÖNEN
Prof. Refik MOLVA
Dr. Alain PANNETRAT

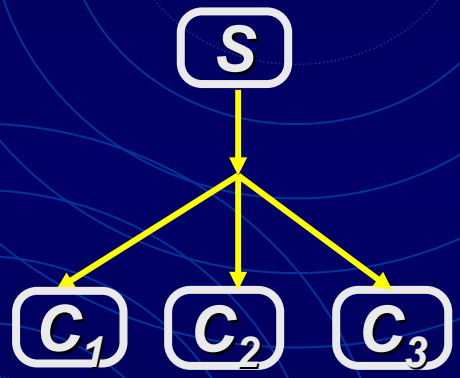
4 Juillet 2002

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

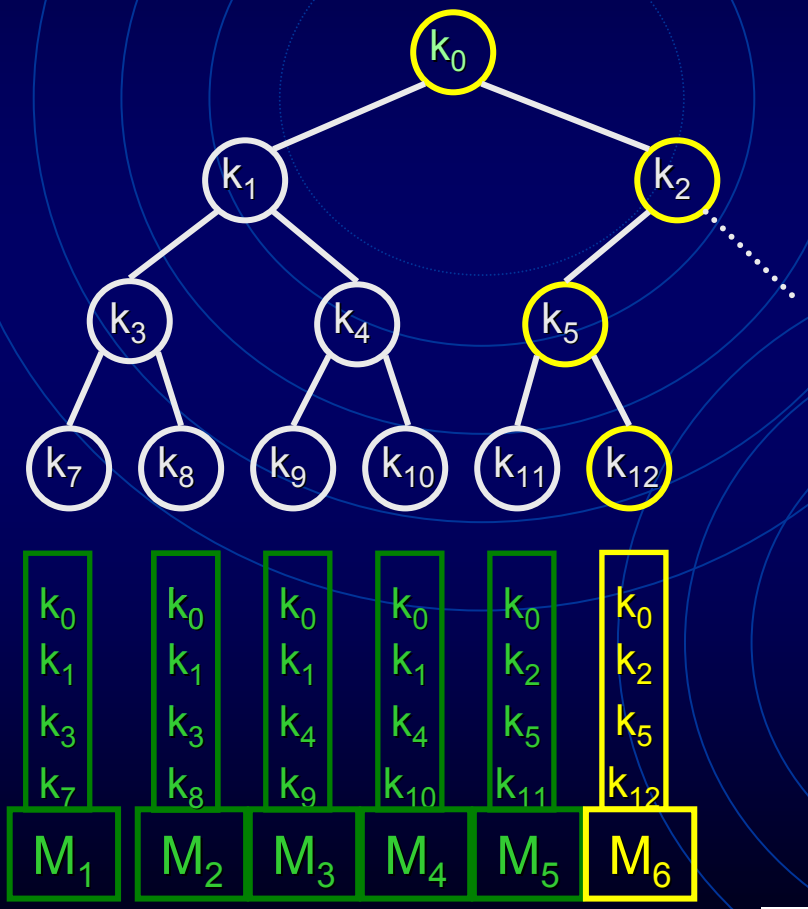
Définitions et besoins (2/2)

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

Confidentialité et Distribution des clefs

- Les besoins
  - 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)

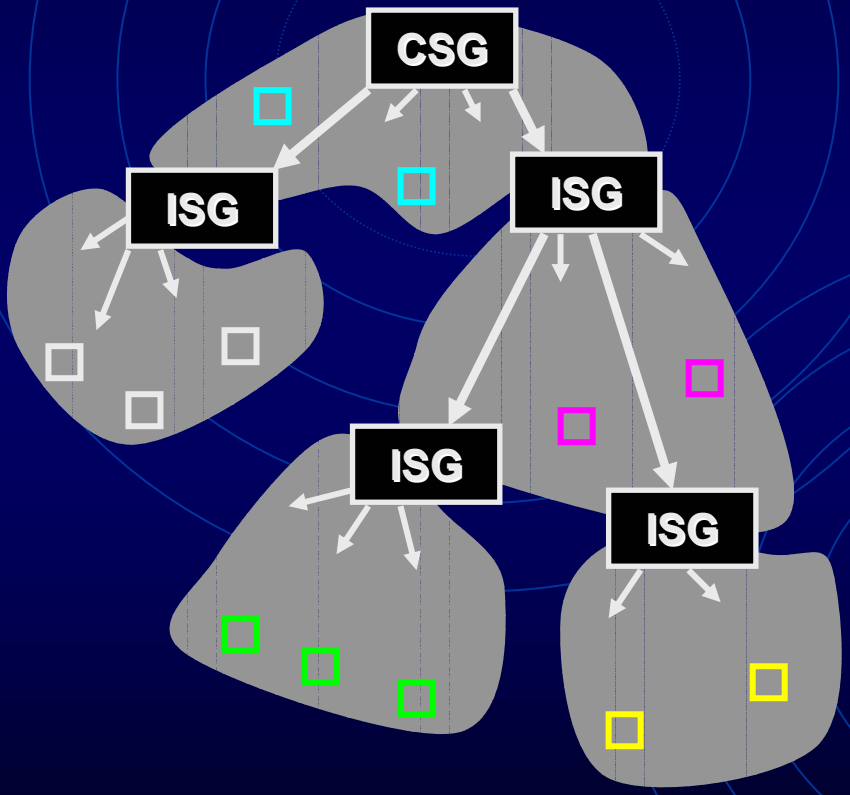
Les arbres de clefs hiérarchiques



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

- Inconvénients :
  - endiguement;
  - problème de robustesse

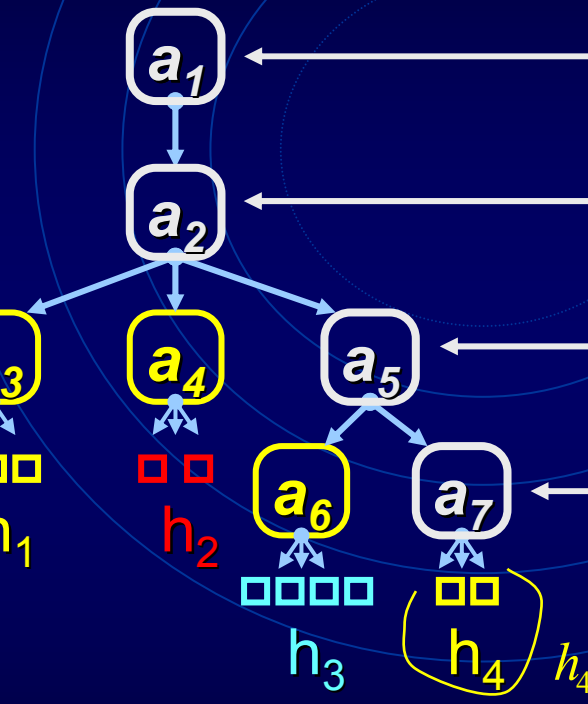
Les arbres de rechiffrement



•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

Une technique asymétrique : $f(x) = x^a \bmod N$



La source envoie:
$S_1 = (S_0)^{a_1} \bmod N$

L'intermédiaire envoie:
$S_2 = (S_1)^{a_2} \bmod N$

L'intermédiaire envoie:
$S_3 = (S_2)^{a_5} \bmod N$

L'intermédiaire envoie:
$S_4 = (S_3)^{a_7} \bmod N$

$h_4(x) = x^B \bmod N,$

$B = 1/(a_1.a_2.a_5.a_7) \bmod \varphi(N)$

$h_4(S_4) = S_0$

- Avantages :
  - échelonnabilité
  - endiguement ;
  - pas de confiance aux nœuds intermédiaires
- Inconvénients :
  - coût de calcul
  ⇒ pas utile pour le chiffrement de paquets
  ⇒ utilisable pour la distribution de clefs

Une deuxième solution

M = 01010101101111010111101…

⊕

$P(k_1)$ = 10100100100100010111 1…

⊕

$P(k_2)$ = 10100001000101110000000 1…

⊕

$P(k_3)$ = 10100001000101110000000 1…

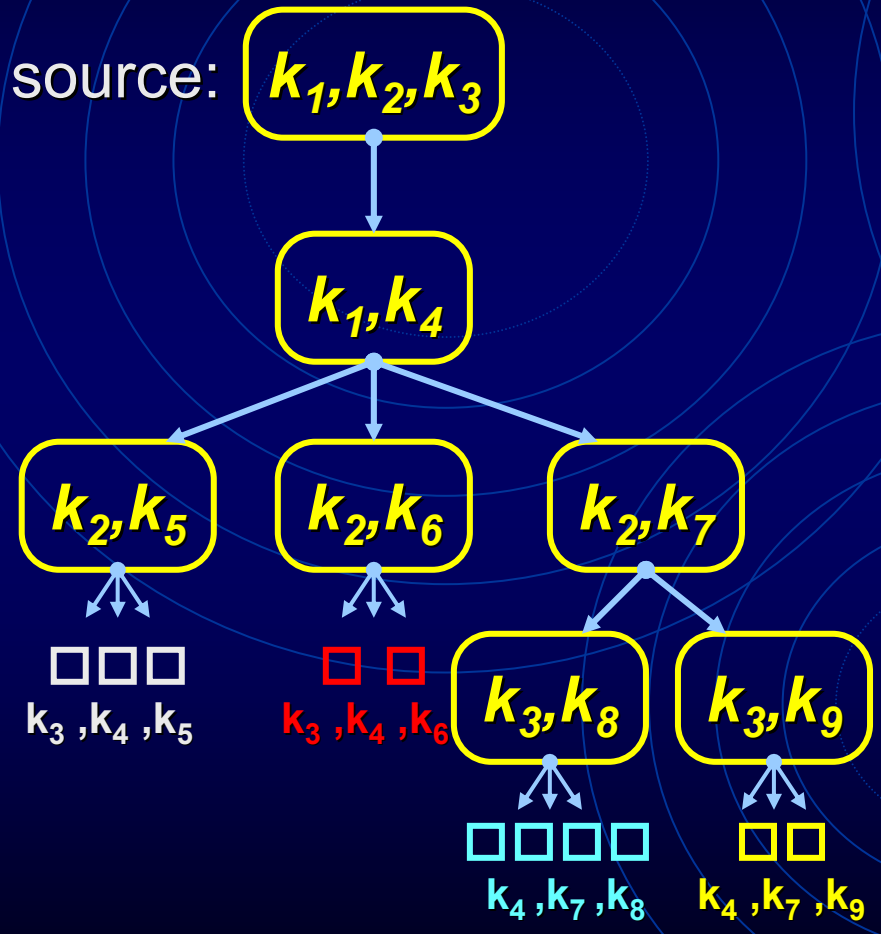
C = 11110001001011110101 0010…

$C = M \oplus P(k_1) \oplus P(k_2) \oplus P(k_3)$ $C' = M \oplus P(k_1) \oplus P(k_4) \oplus P(k_3)$

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

intermédiaire

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.

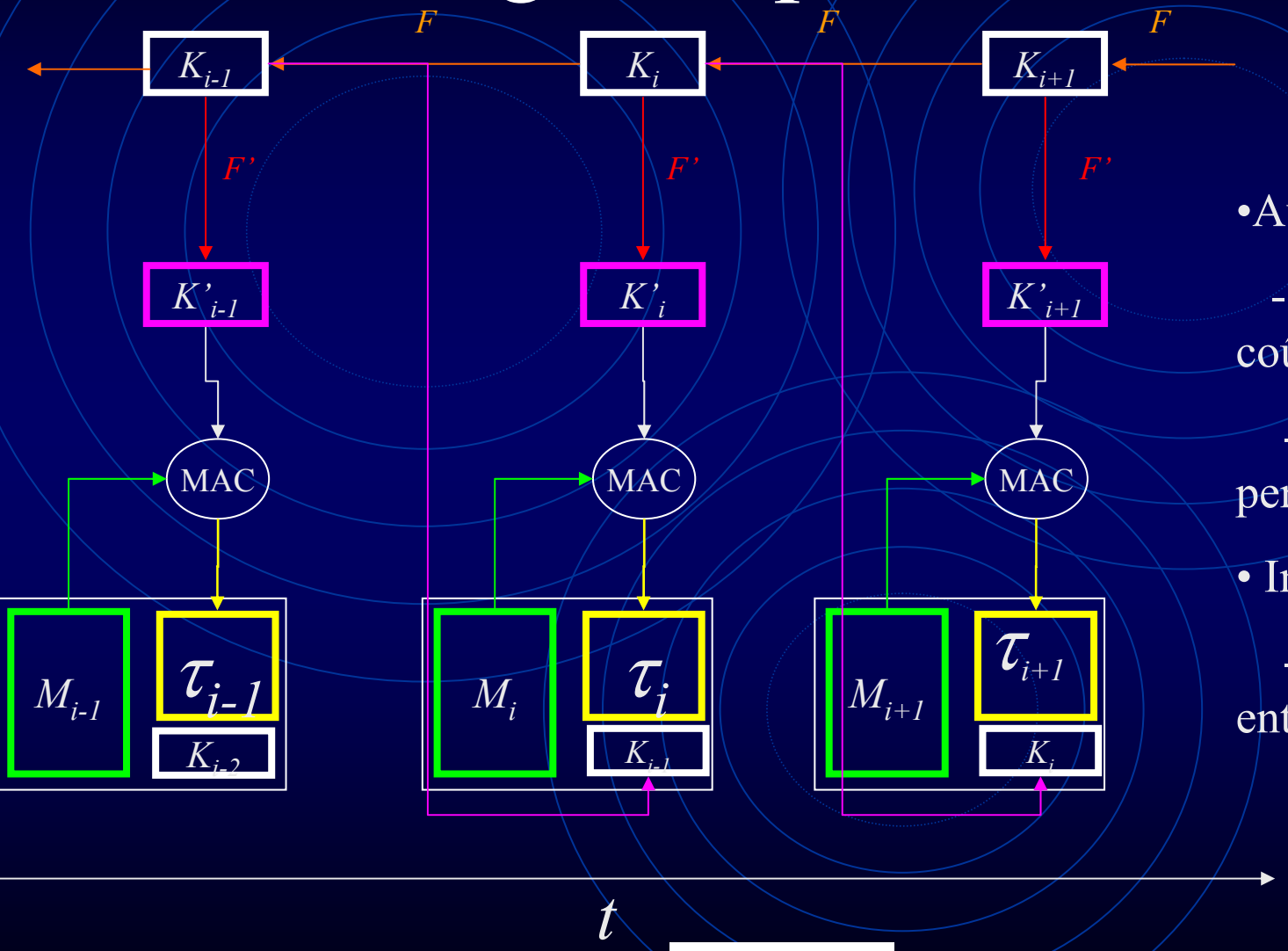
Authentification multicast

- 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 :

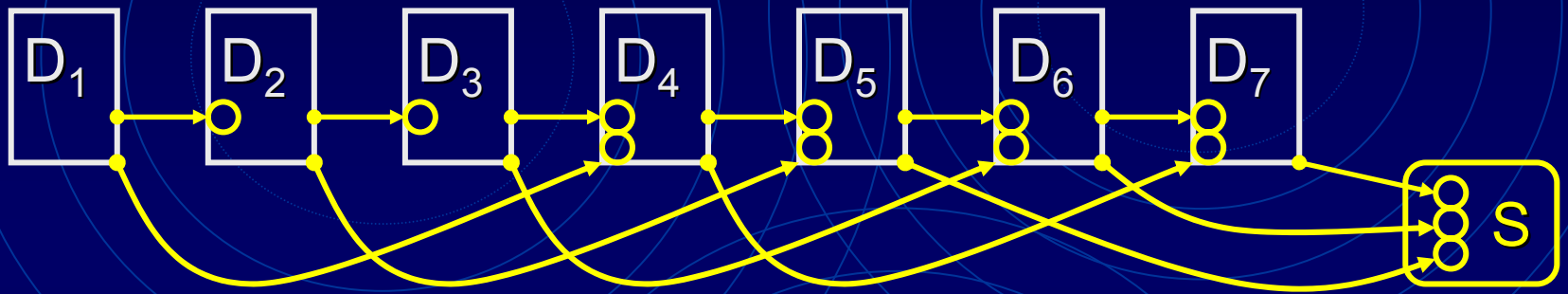
- opérations non coûteuses

- tolérance aux pertes

• Inconvénient :

- synchronisation entre S et C

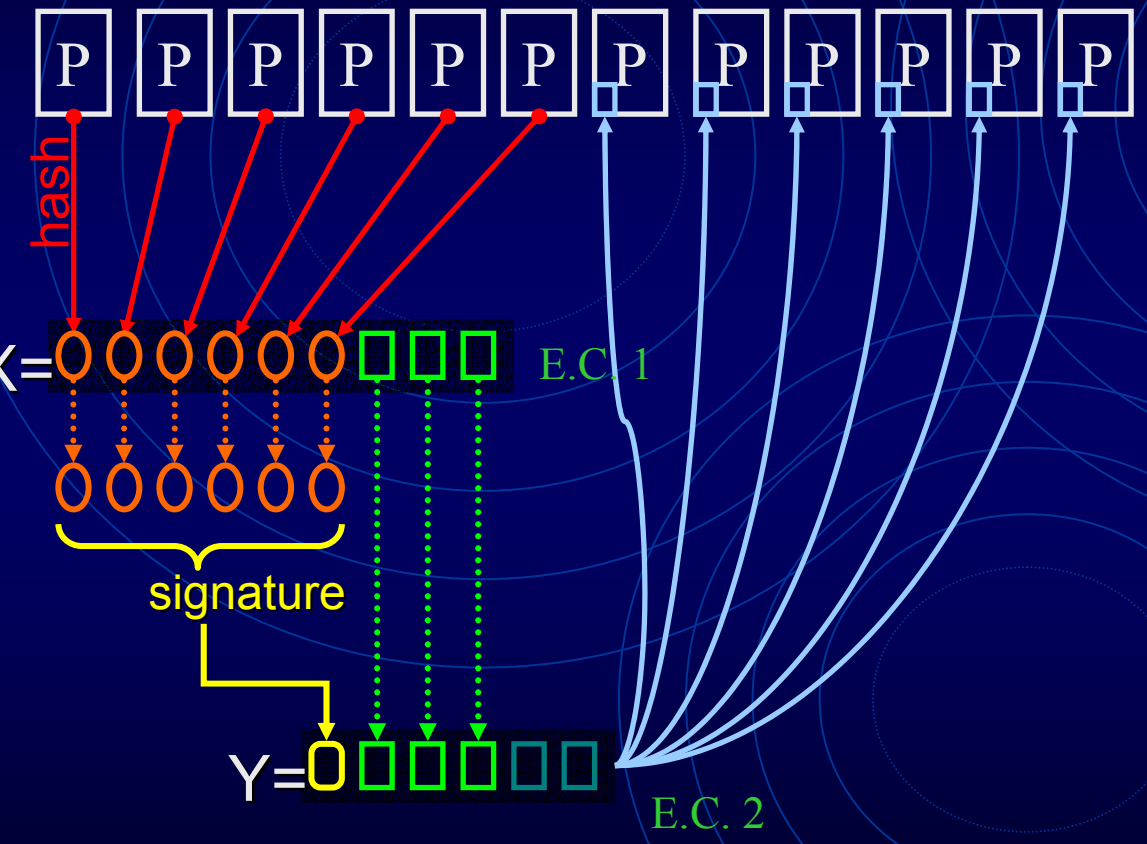
Chaînages par hachages :EMMS



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

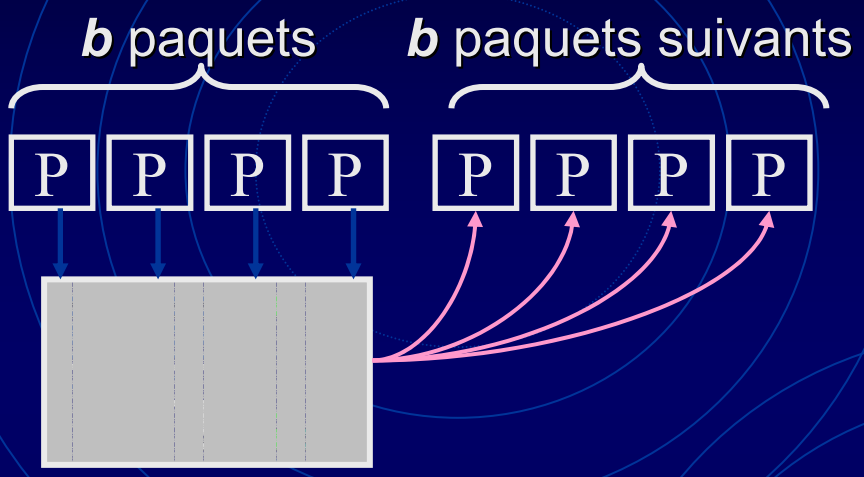
• Inconvénients :
- “comment calculer la taille *b* d’un bloc ?”

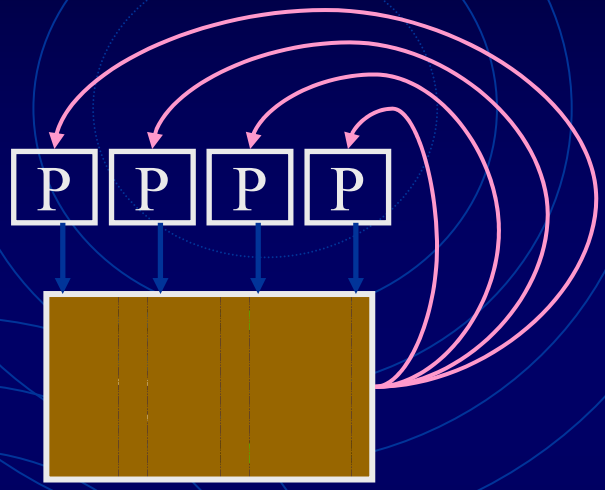
Utilisation des FECs

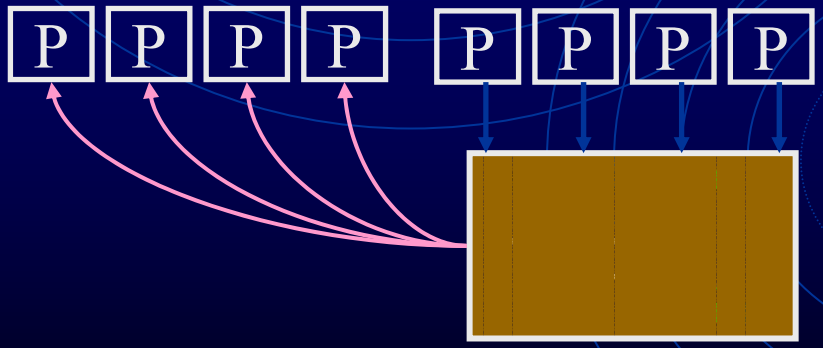


- Avantages :
  - réduction du coût de la signature
  - tolérance aux pertes
- Inconvénients :
  - calcul des codes reconstructeurs

3 modes







Influence:

- Tampon serveur
- Délai d'authentification

Conclusion

- Etat de l'art sur deux besoins de sécurité :
  - Confidentialité
    - Une clef de groupe similaire pour tous les membres
    - Une clef de sous-groupe locale : noeuds intermédiaires
  - Authentification
    - Chaînage des MACs de messages au cours du temps
    - Chaînage des hachages
    - Utilisation des codes correcteurs d'erreurs.

Références

- *"Secure group communications using key graphs",* Wong, Gouda, Lam,1998.
- *"Iolus : A framework for scalable secure Multicasting",* Mittra,1997.
- *"Scalable multicast security with dynamic recipient groups",* Molva, Pannetrat, 2000.
- *"Multiple Layer encryption for Multicast groups",* Pannetrat,Molva, 2002.
- *"Efficient authentication and signing of multicast streams over lossy channels",* Perrig, Canetti, Tygar and Song,2000.
- *"Real time multicast packet authentication",* Pannetrat, Molva 2002.