Protection contre l'analyse du trafic dans la Voix sur IP

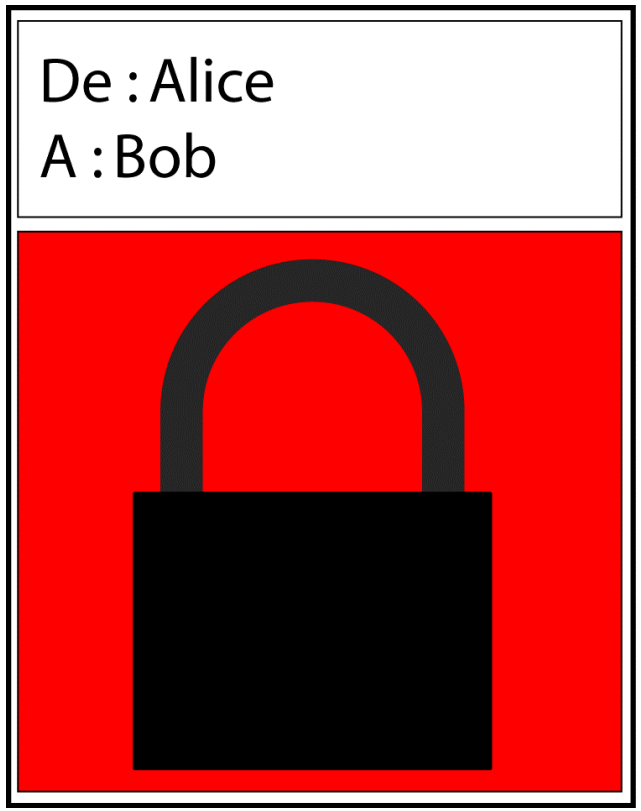
Carlos AGUILAR MELCHOR
Groupe SeFSI, XLIM, Limoges
Yves DESWARTE
Groupe TSF, LAAS-CNRS, Toulouse

Novembre 2006

Plan

- Problématique
  - Protection des méta-données
  - Approche classique sur IP
  - Cadre de travail
- Solutions
  - Primitives
  - Solutions basées sur la diffusion
  - Le pMIX et ses variantes
- Synthèse et perspectives

Protection des méta-données :
Méta-données sur IP (1/2)



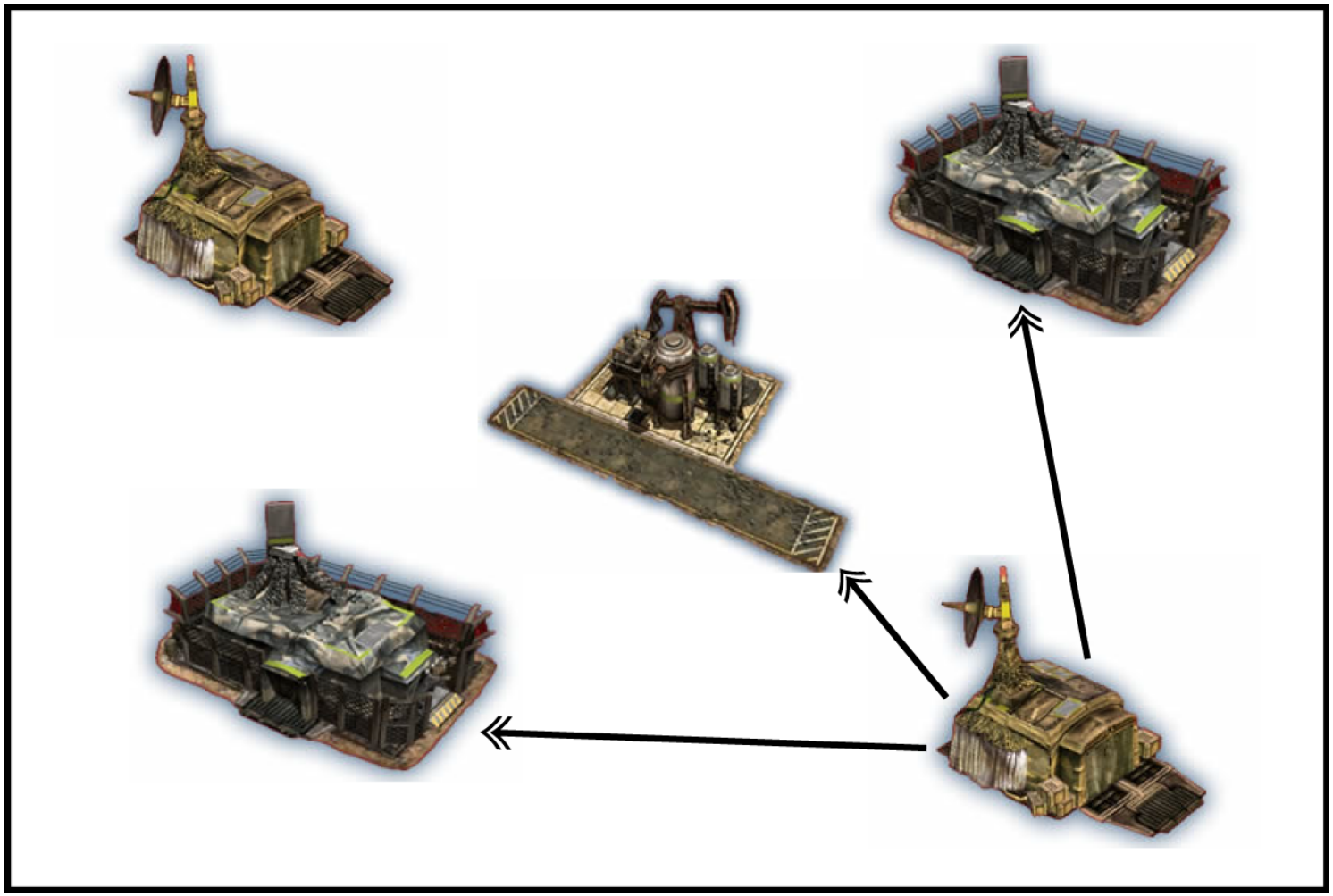
- Un attaquant peut s'intéresser :
  - au contenu d'un message;
  - à son en-tête;
  - à son existence.
- Il est possible de chiffrer le contenu d'un message
- Son en-tête ne peut pas être chiffrée
- Le message ne peut pas être occulté

Protection des méta-données : Méta-données sur IP (2/2)

- Contexte des communications
  - Qui communique avec qui
  - Quand un utilisateur communique
  - Nombre de communications dans un réseau

- Problèmes de sécurité
  - Localisation
  - Inférence sur le contenu
  - etc.

Protection des méta-données :
Exemples : localisation d'un officier

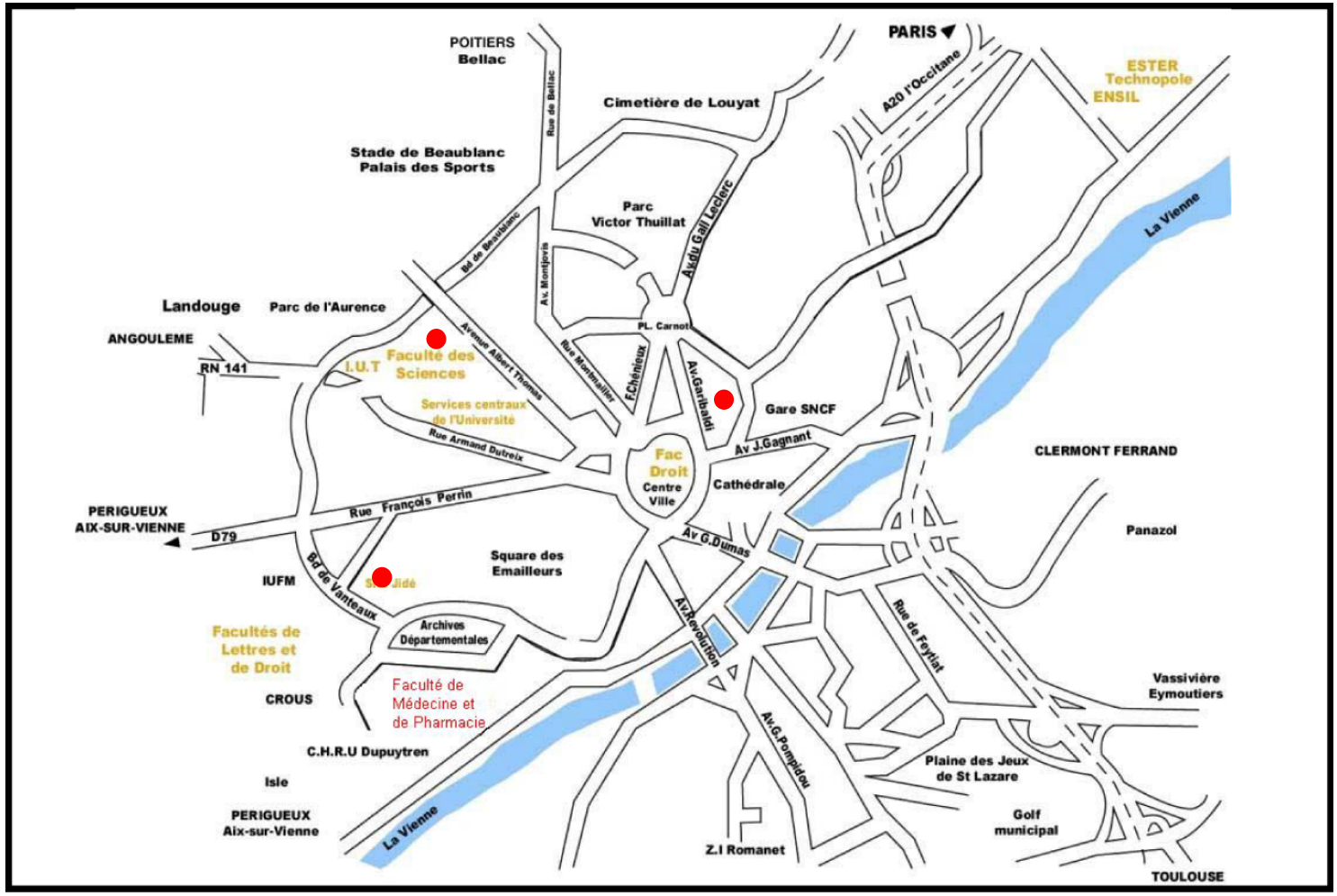


Protection des méta-données :
Exemples : localisation dans un bâtiment

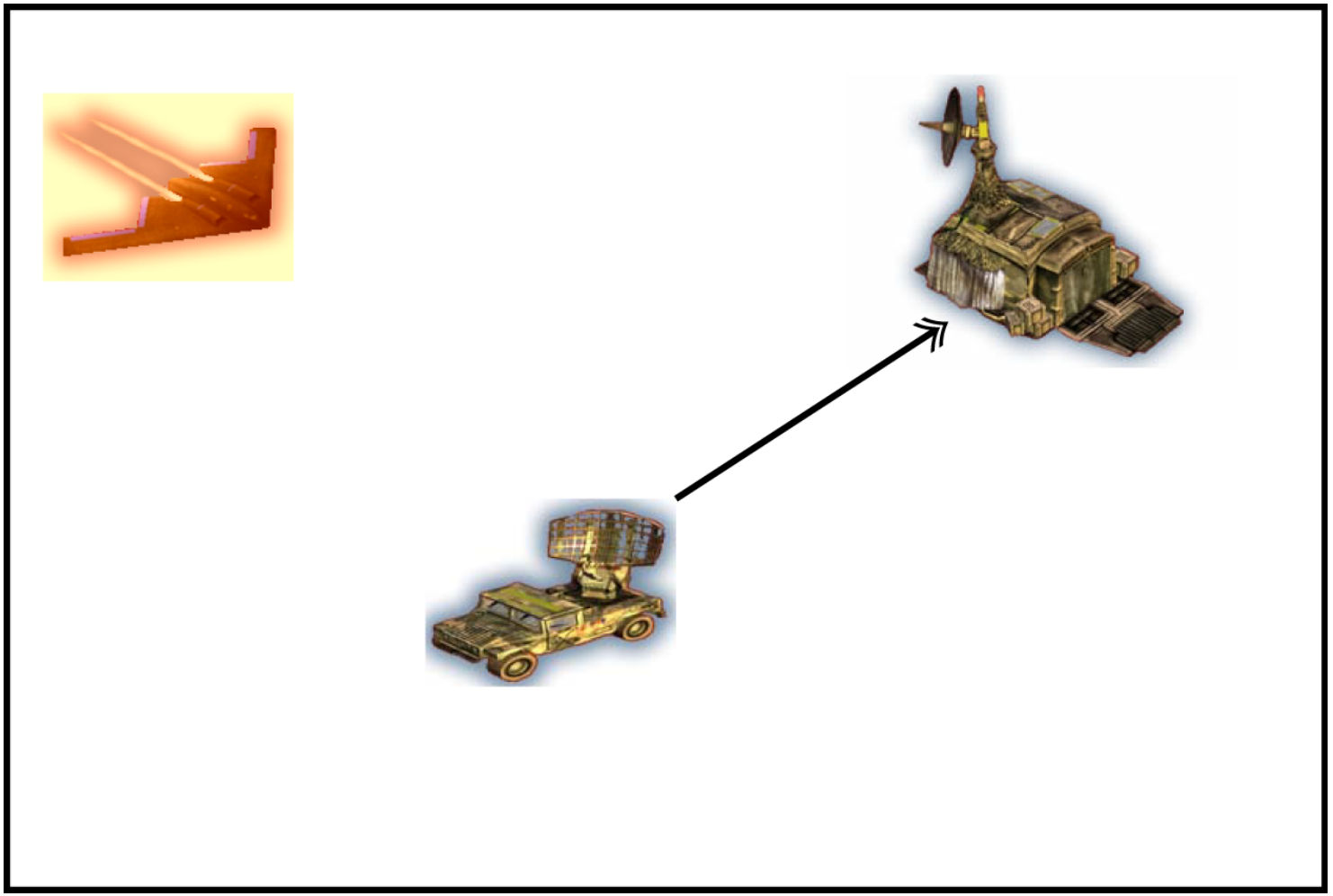
Bâtiments sensibles

Ecoutes internes

Protection des méta-données :
Exemples : localisation entre plusieurs sites



Protection des méta-données :
Exemples : Inférence d'un repérage RADAR

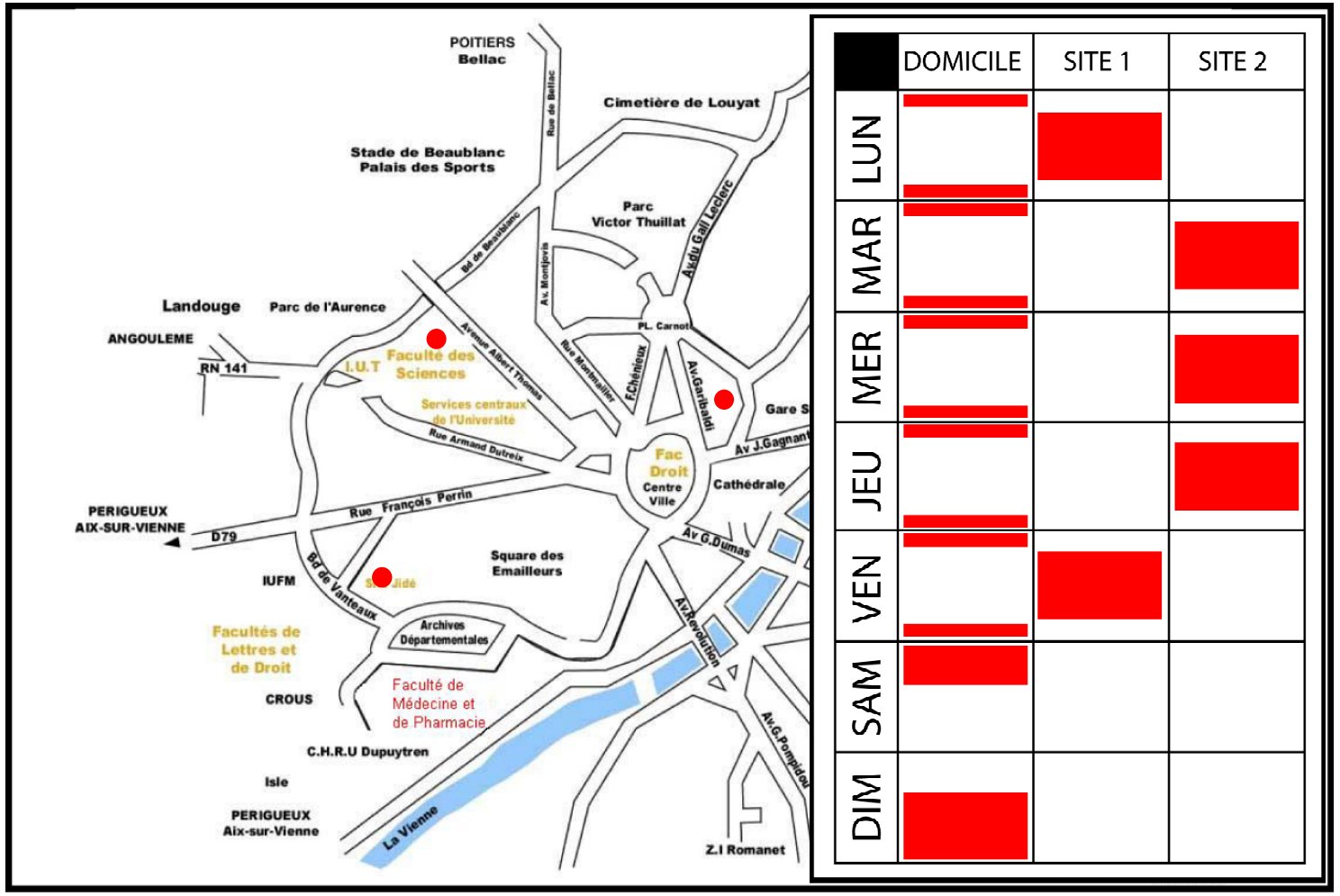


Protection des méta-données :
Exemples : Inférence des activités

Bâtiments sensibles

Ecoutes internes

Protection des méta-données :
Exemples : Inférence des habitudes



	DOMICILE	SITE 1	SITE 2
LUN			
MAR			
MER			
JEU			
VEN			
SAM			
DIM			

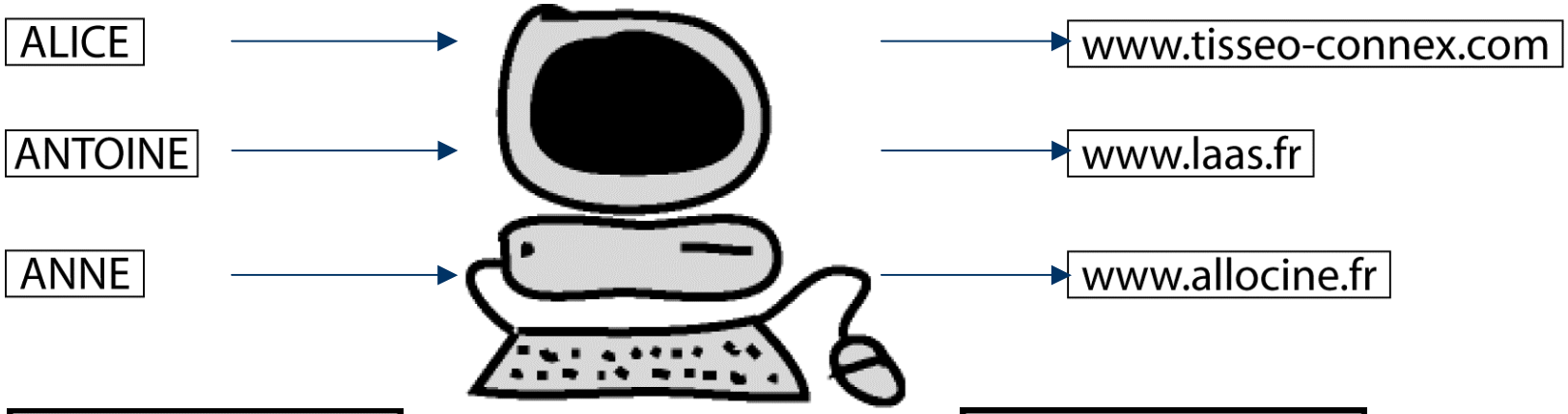
Protection des méta-données : Performances requises pour la Voix sur IP

- Latence maximale d'aller-retour de 250ms
- Bande passante de 8 à 32 Kbits/s (codecs G729-EV)

Plan

- Problématique
  - Protection des méta-données
  - Approche classique sur IP
  - Cadre de travail
- Solutions
  - Primitives
  - Solutions basées sur la diffusion
  - Le pMIX et ses variantes
- Synthèse et perspectives

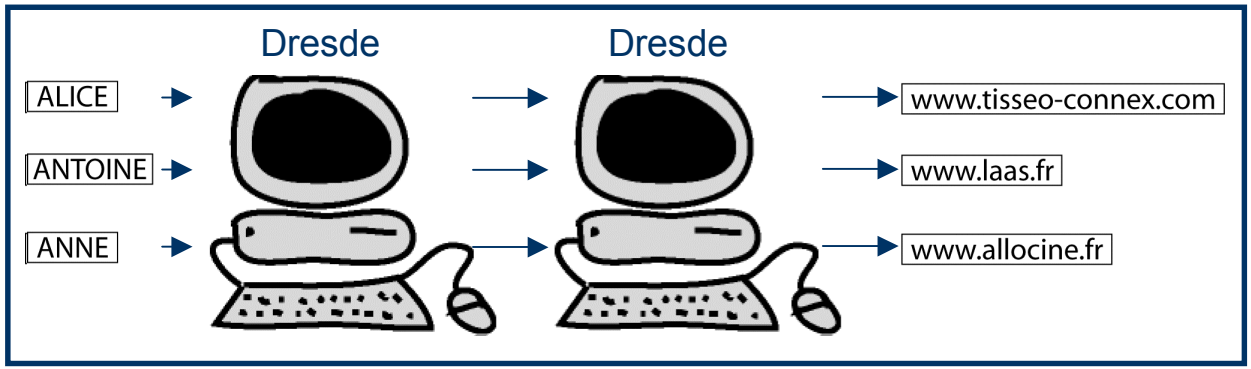
Approche classique sur IP :
L'utilisation de relais



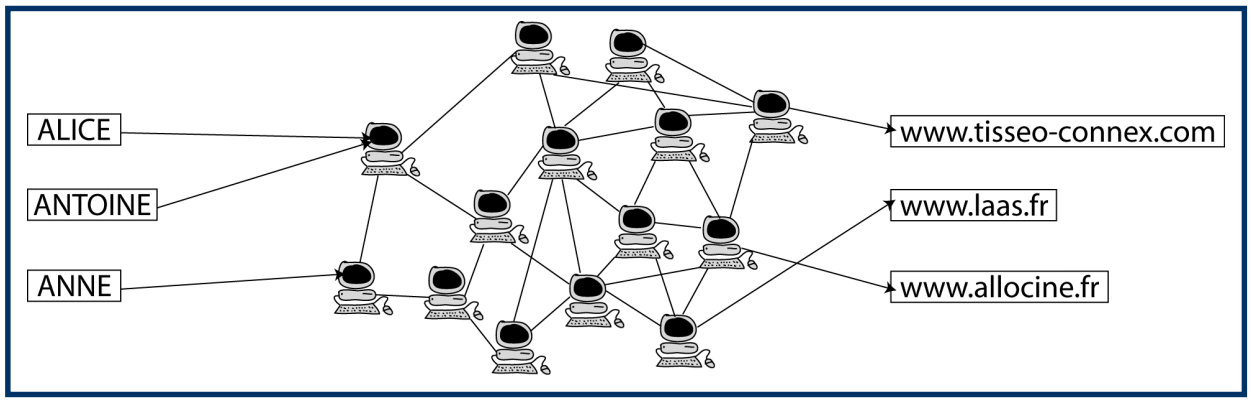
- Déchiffre
- Cumule
- Désordonne
- Relaye

Approche classique sur IP :
Cascades et réseaux

Cascade : JAP
http://anon.inf.tu-dresden.de



Réseau : TOR
http://tor.eff.org



Plan

- Problématique
  - Protection des méta-données
  - Approche classique sur IP
  - Cadre de travail
- Solutions
  - Primitives
  - Solutions basées sur la diffusion
  - Le pMIX et ses variantes
- Synthèse et perspectives

Cadre de travail

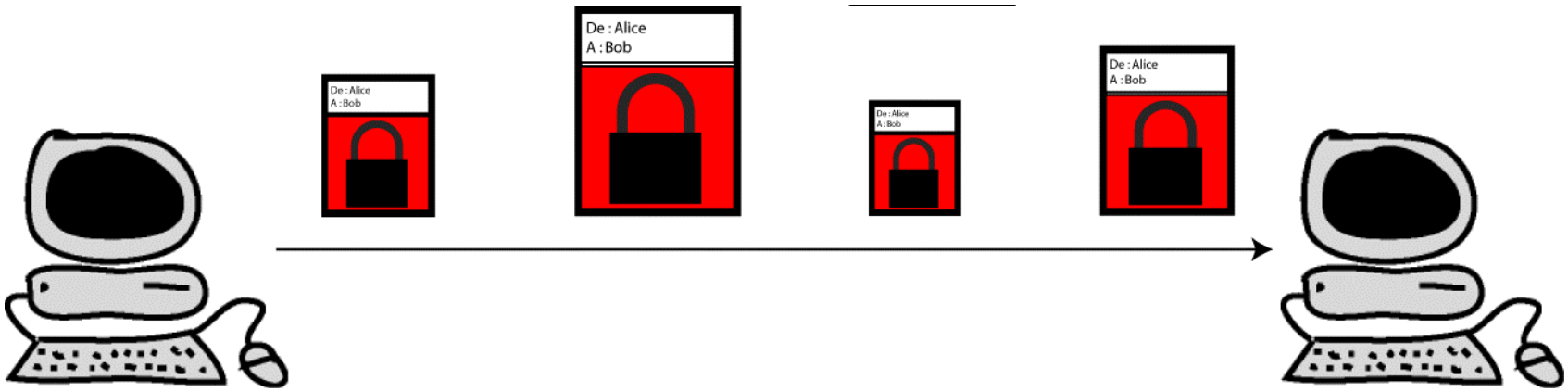
- Utilisation d'un seul relais
  - Nombre d'utilisateurs limité

- Observateur global : peut écouter tous les liens
  - Dans nos hypothèses, il est plausible
    - non-observabilité en émission
    - non-observabilité en réception

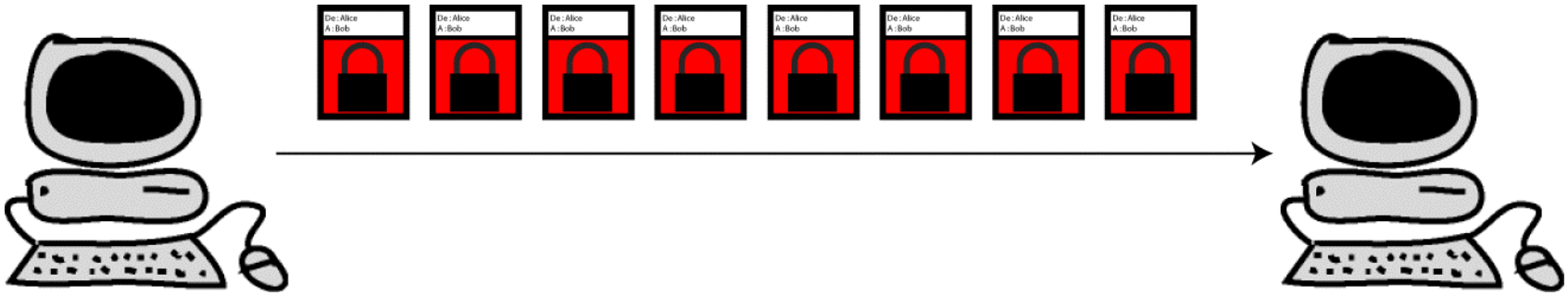
Plan

- Problématique
  - Protection des méta-données
  - Approche classique sur IP
  - Cadre de travail
- Solutions
  - Primitives
  - Solutions basées sur la diffusion
  - Le pMIX et ses variantes
- Synthèse et perspectives

Primitives :
Le bourrage chiffré

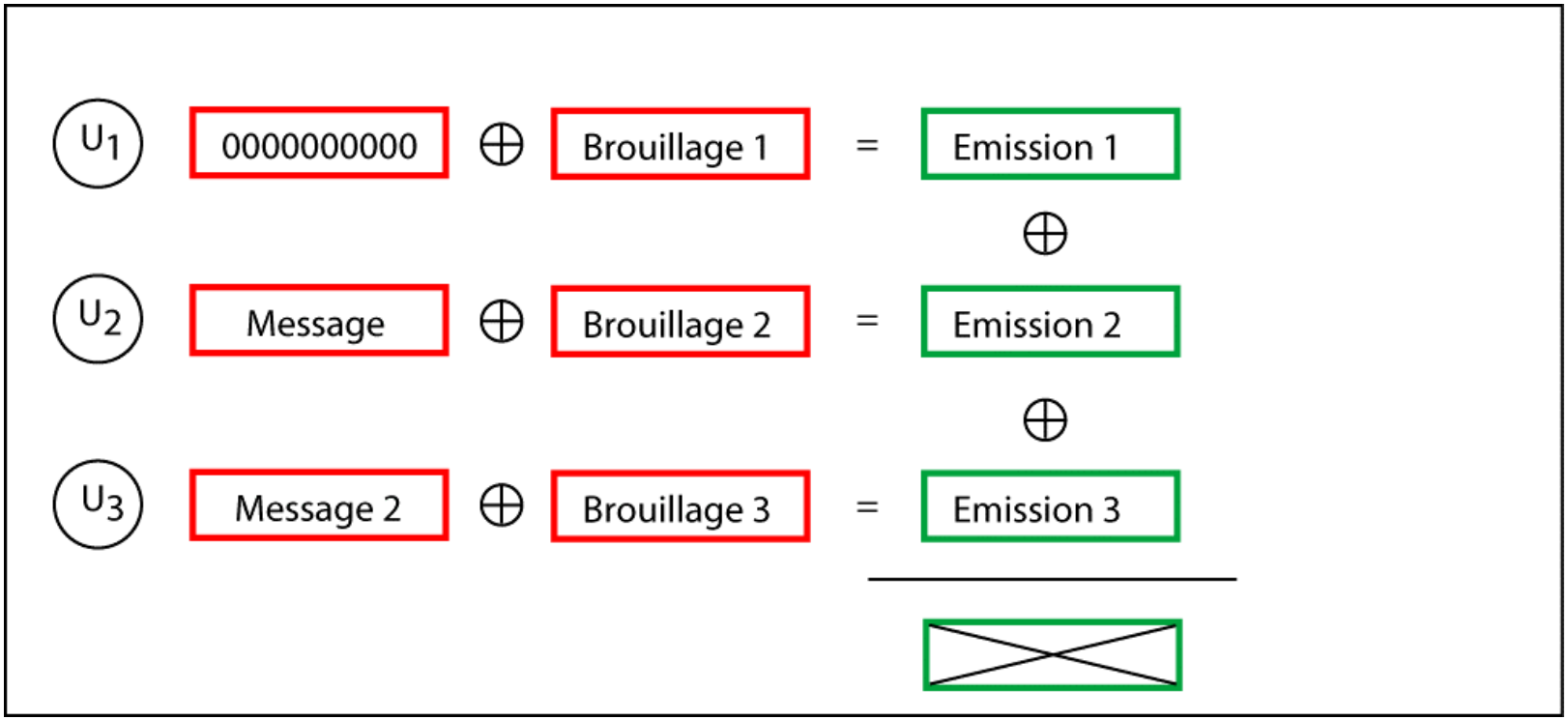


Primitives :
Le bourrage chiffré



- L'utilisation de bourrage chiffré
  - émettre à des intervalles réguliers des messages chiffrés de taille constante,
  - contenant soit des messages, soit du bruit

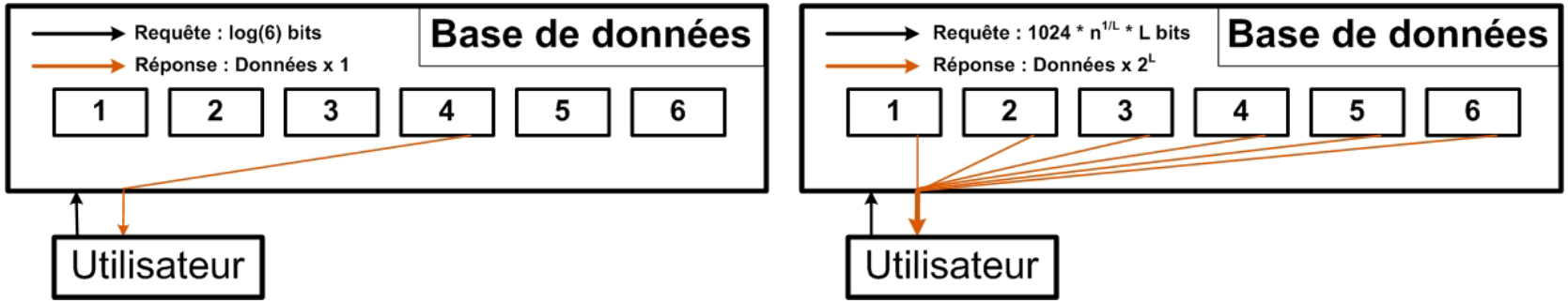
Primitives :
L'envoi superposé



Primitives :
La diffusion avec adressage implicite

- Envoyer les messages à tout un réseau
- Inclure une marque pour que chaque destinataire reconnaisse les messages qui lui sont destinés

Primitives :
Les protocoles PIR



- Permettent de récupérer un objet
  - Sans indiquer lequel c'est
  - Avec un petit facteur d'expansion (≤ 2)
- Pour remplacer la diffusion avec adressage implicite
  - Utilisateurs non-observables en réception
  - Diminue radicalement le coût des communications
  - Augmente fortement le coût calculatoire
- Possibilité de mise sous séquestre des clés

Primitives :
Combinaison des primitives

- Utilisation de serveurs
- Non-observabilité en émission et en réception

	Diffusion	PIR
Bourrage chiffré	EBBS	pMIX
Envoi superposé	Serveur DC-net	**pDCnet**

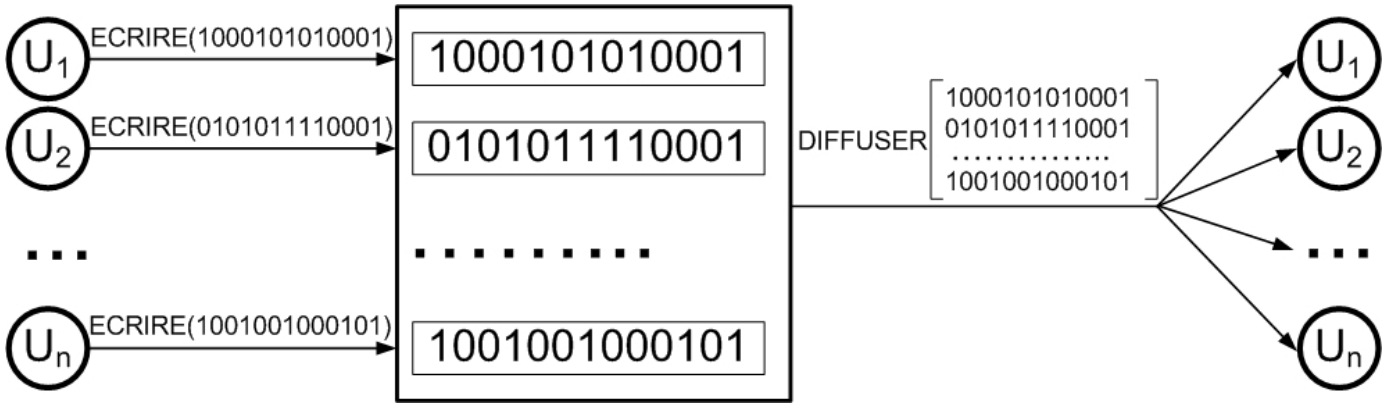
Plan

- Problématique
  - Protection des méta-données
  - Approche classique sur IP
  - Cadre de travail
- Solutions
  - Primitives
  - Solutions basées sur la diffusion
  - Le pMIX et ses variantes
- Synthèse et perspectives

Solutions basées sur la diffusion : Cas d'étude : Voix sur IP

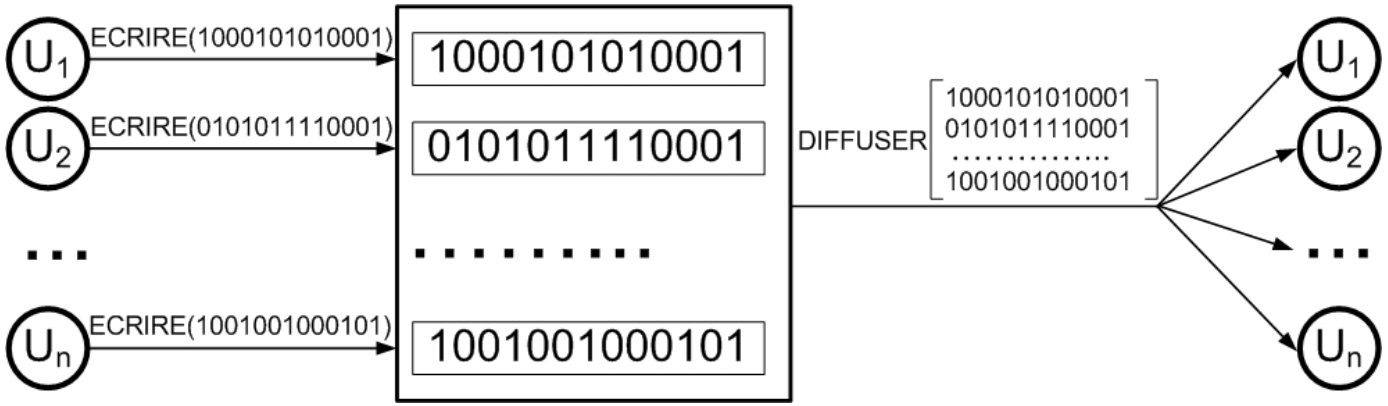
- Canal de communication pour VoIP : 10 Kbits/s
- Limitation du coût pour les clients :
  - ≤ 10 % de leur bande passante disponible
  - Dans tout les cas, ≤ 1 Mbit/s
- Réseau local : bande passante 100 Mbit/s
- Internet
  - ADSL 1 Mbit/s en réception, 128 Kbits/s en émission
  - UMTS 384 Kbits/s en réception, 64 Kbits/s en émission

Solutions basées sur la diffusion : L'EBBS (1/2)



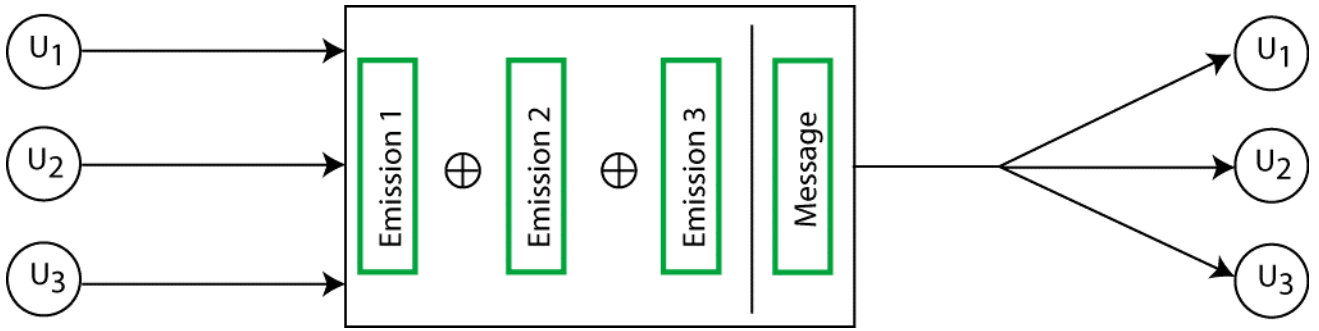
- Un emplacement par utilisateur
- Utilisation de bourrage chiffré
- Émission par tours

Solutions basées sur la diffusion : L'EBBS (2/2)



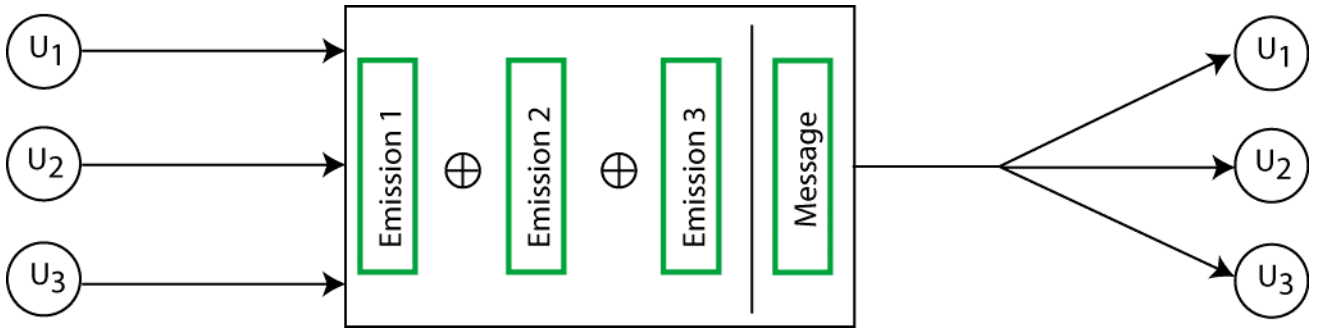
- Messages émis par les clients : **1**
- Messages reçus par les clients : **n**
- Messages émis par le serveur : **n** ou **n^2**
- Utilisateurs : **10(WAN)/100(LAN)**

Solutions basées sur la diffusion : Le serveur DC-net (1/2)



- Collaboration d'agents asynchrones et indépendants
  - Évaluation difficile théoriquement
  - Implémentation pratique nécessaire
  - Étude de performances
- Expérimentation la plus générale possible
  - Bornes supérieures en performance : grappe d'ordinateurs
  - Plus réaliste : dans le réseau du LAAS-CNRS

Solutions basées sur la diffusion : Le serveur DC-net (2/2)



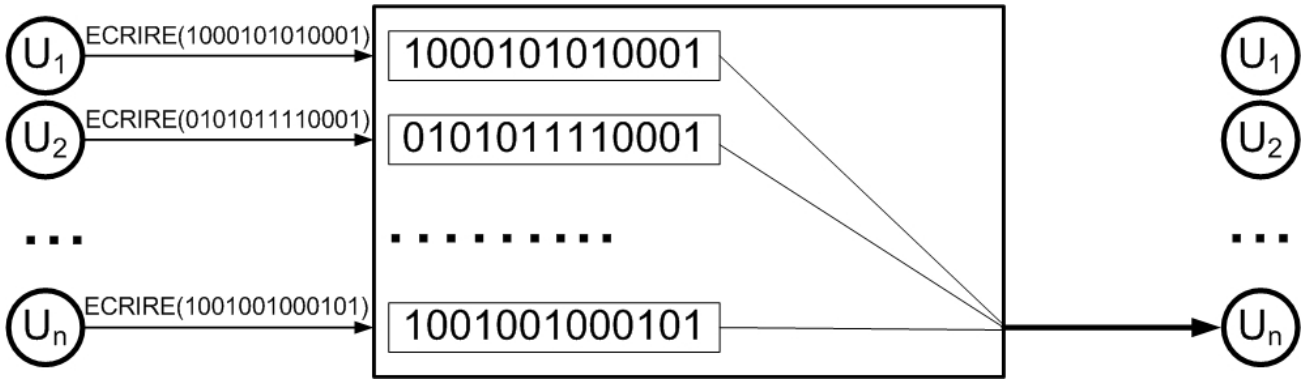
- Messages émis par les clients : **m**
- Messages reçus par les clients : **m**
- Utilisateurs : **centaines**

- **Inutilisable sur des réseaux à grande échelle**

Plan

- Problématique
  - Protection des méta-données
  - Approches classiques sur IP
  - Cadre de travail
- Solutions
  - Primitives
  - Solutions basées sur la diffusion
  - Le pMIX et ses variantes
- Synthèse et perspectives

Le pMIX et ses variantes :
Le pMIX (1/3)

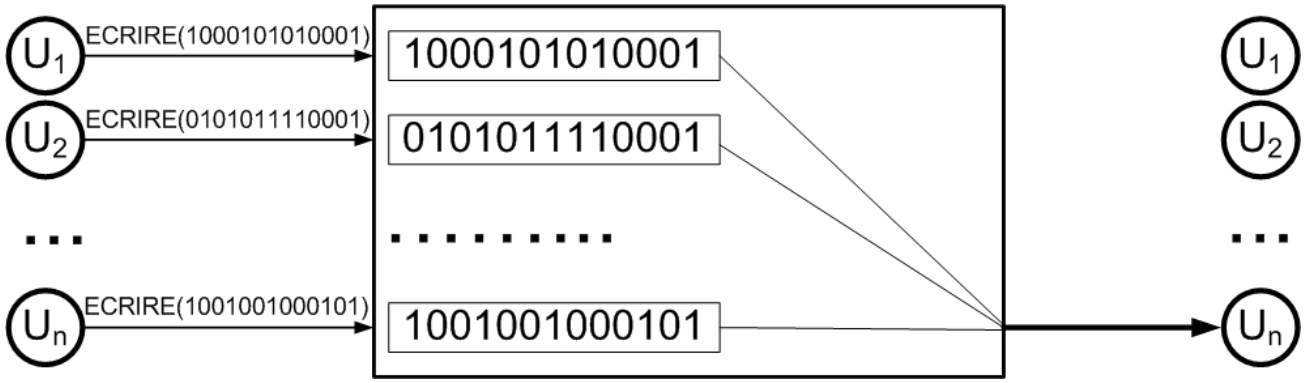


- Coût d'une réponse PIR proportionnel à la taille de la base de données
  - Proportionnelle au nombre d'utilisateurs
- Nombre de réponses proportionnel au nombre d'utilisateurs

⇒ Coût calculatoire par tour en $\mathbf{n^2}$

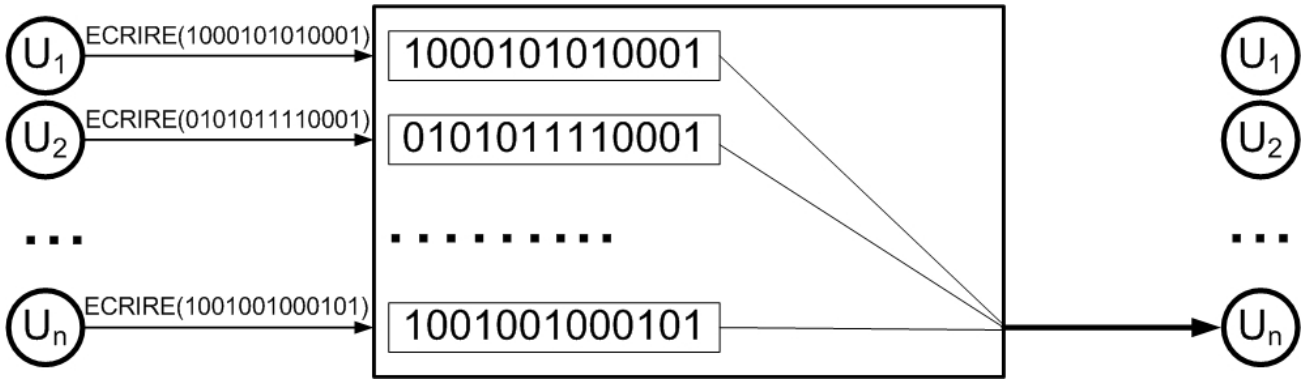
- Coût par bit : multiplication modulaire
  - Propre aux protocoles PIR actuels et pas au pMIX

Le pMIX et ses variantes :
Le pMIX (2/3)



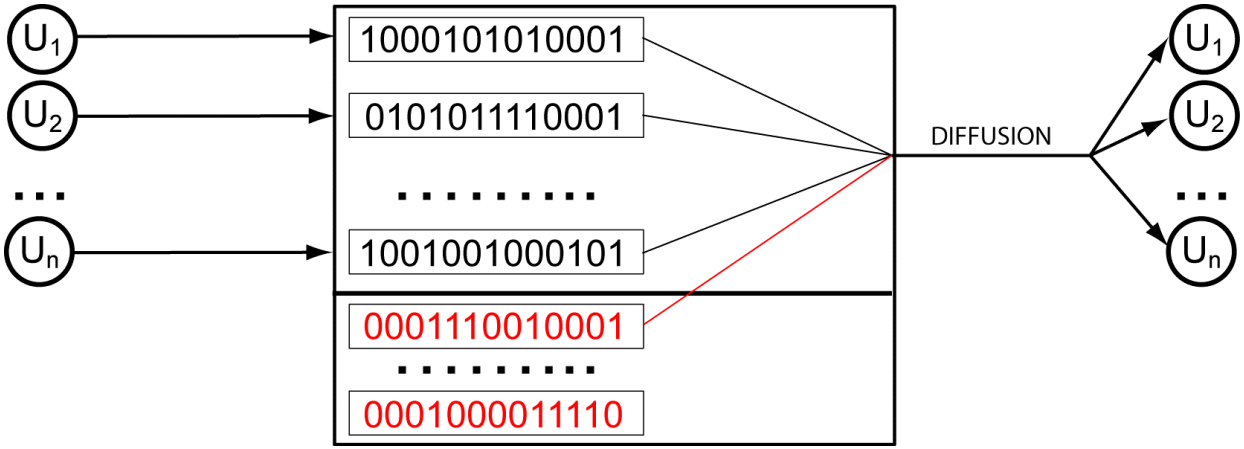
- Le débit augmente linéairement avec la puissance de calcul
- Coût calculatoire prohibitif pour plus de quelques dizaines d'utilisateurs
- Protocole PIR rapide (en cours)
  - jusqu'à 250 utilisateurs avec un processeur actuel

Le pMIX et ses variantes :
Le pMIX (3/3)



- Messages émis par les clients : **1**
- Messages reçus par les clients : **1 (de taille F)**
- Utilisateurs : **~10**

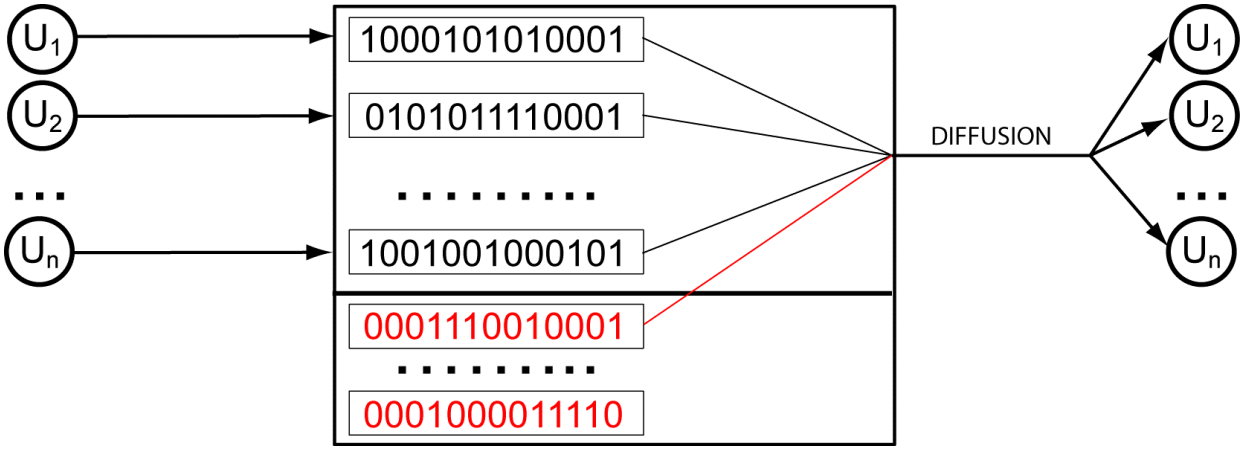
Le pMIX et ses variantes :
L'apMIX (1/3)



- Réduction du nombre de requêtes à **m**
- Coût calculatoire : **n x m**
- IEEE Symposium on Network Computing and Applications, Boston, MA, 2006

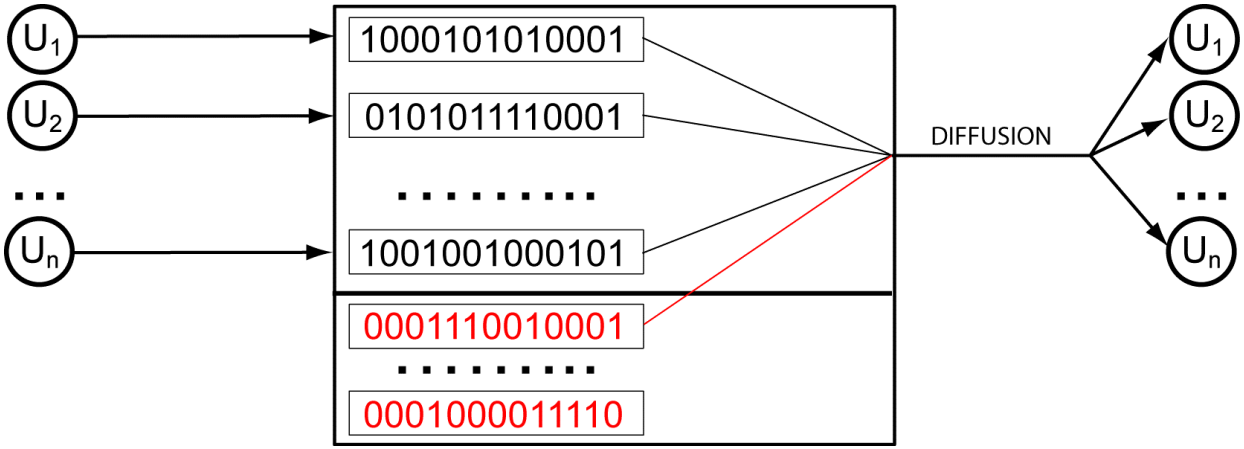
  Aguilar Melchor and Deswarte "pMIX variants"

Le pMIX et ses variantes :
L'apMIX (2/3)



- 1 UC :
  - 50 Clients, 1 Communication simultanée
  - 25 Clients, 2 Communications simultanées
- 4 UCs :
  - 50 Clients, 4 Communications simultanées
  - 200 Clients, 1 Communication simultanée

Le pMIX et ses variantes :
L'apMIX (3/3)



- Environ 10 euros par client et communication
  - Prix d'une oreillette avec microphone
- Négligeable devant le prix d'un téléphone VoIP
  - Chiffrement nécessaire
- Induit un coût raisonnable

Plan

- Problématique
  - Protection des méta-données
  - Approches classiques sur IP
  - Cadre de travail
- Solutions
  - Primitives
  - Solutions basées sur la diffusion
  - Le pMIX et ses variantes
- Synthèse et perspectives

Synthèse

- Réseau local
  - Utilisation d'un EBBS si moins de 100 utilisateurs
  - Plus : réseau dédié ou utilisation d'apMIXes

- Internet (ADSL)
  - Seul système utilisable : apMIX
  - Coût raisonnable
  - Difficile au-delà de mil utilisateurs

Perspectives

- Protocoles PIR
  - Amélioration du coût calculatoire
- Implémentation d'un pMIX/apMIX
- Anonymisation de la signalisation