Gestion distribuée d'identités résistante à la Sybil Attack pour un réseau Pair-à-Pair

François Lesueur, Ludovic Mé, Valérie Viet Triem Tong

Supélec, équipe SSIR (EA 4039)

13 juin 2007

Présentation des réseaux P2P

Spécificités des réseaux P2P :

- Forte disponibilité
- Déploiement économique
- Passage à l'échelle
- Équité des pairs
- Absence d'autorité centrale

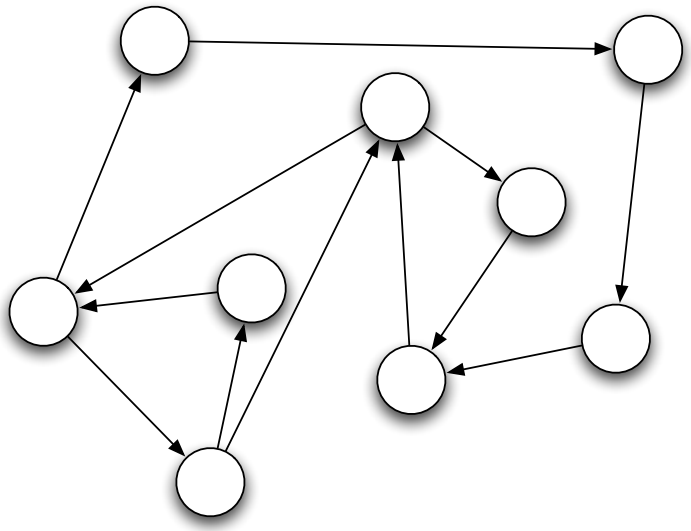
Applications :

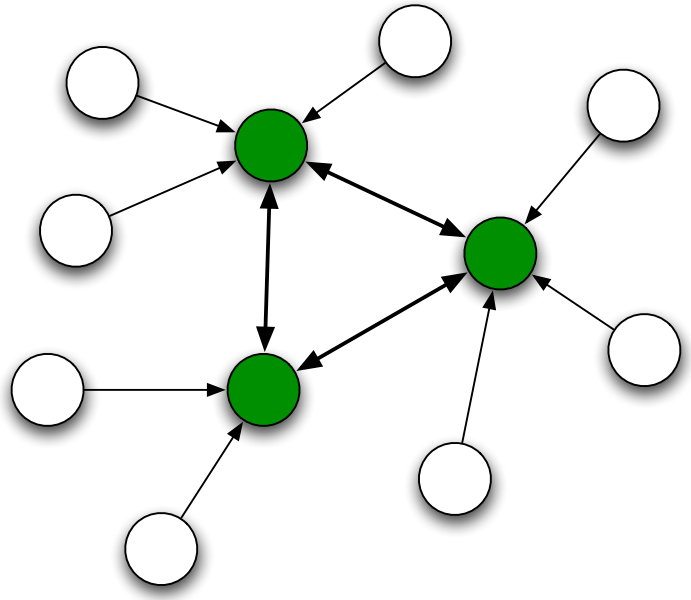
- Partage de fichiers
- Multidiffusion
- Sauvegarde ?

Réseaux P2P non structurés

Les plus connus : Gnutella, Kazaa, Skype

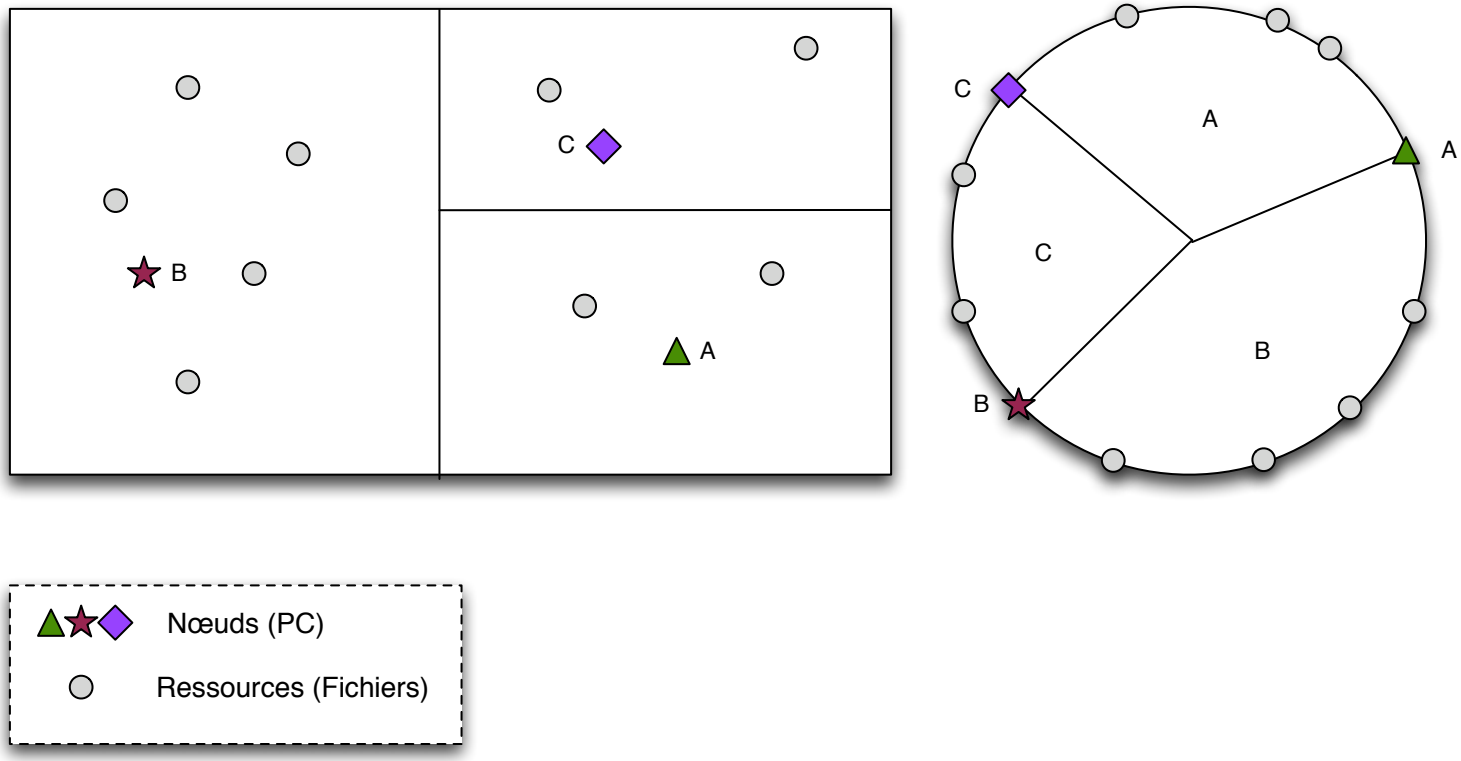
Principe : *Inondation*





Réseaux P2P structurés

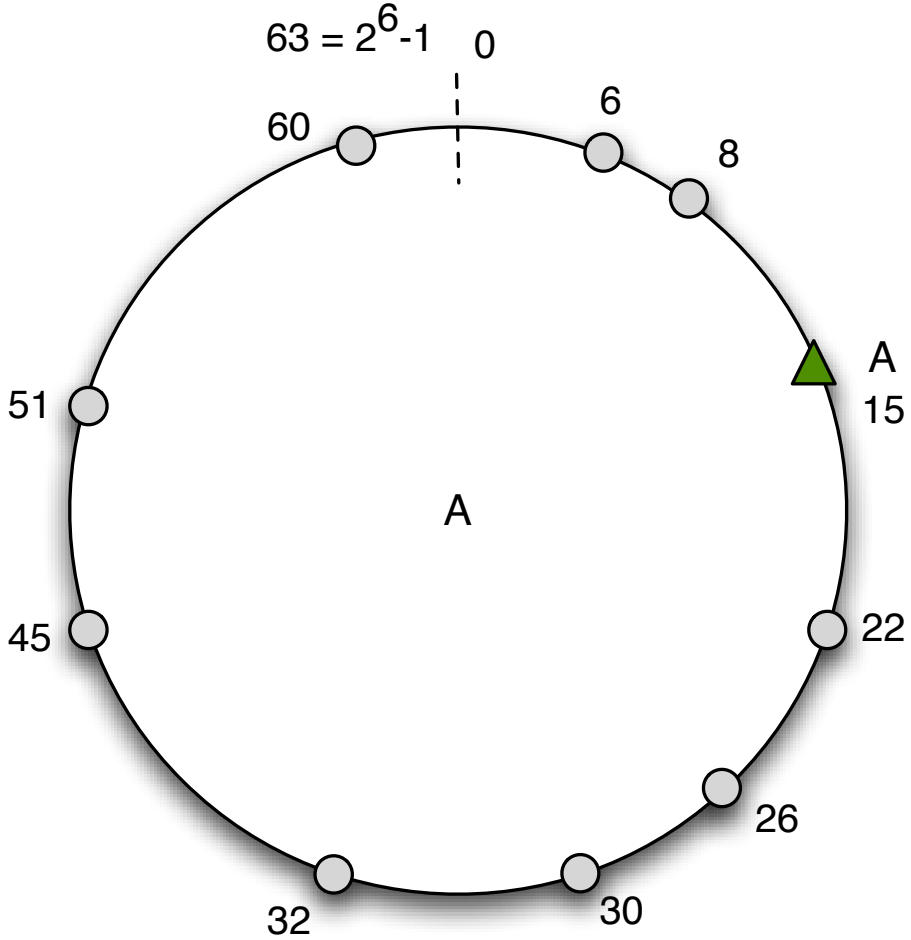
Implémentent une *Distributed Hash Table* (DHT) dans un *overlay*.



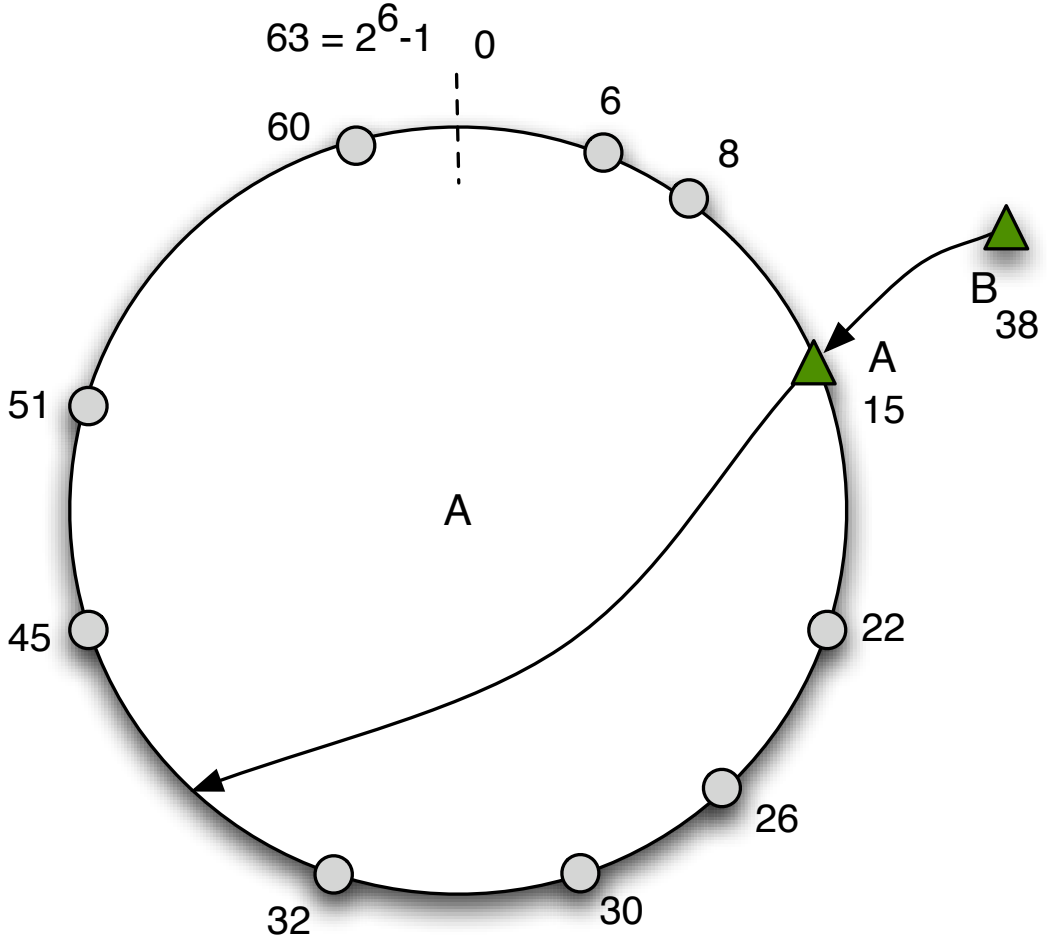
DHT : $key \mapsto value$

Plan

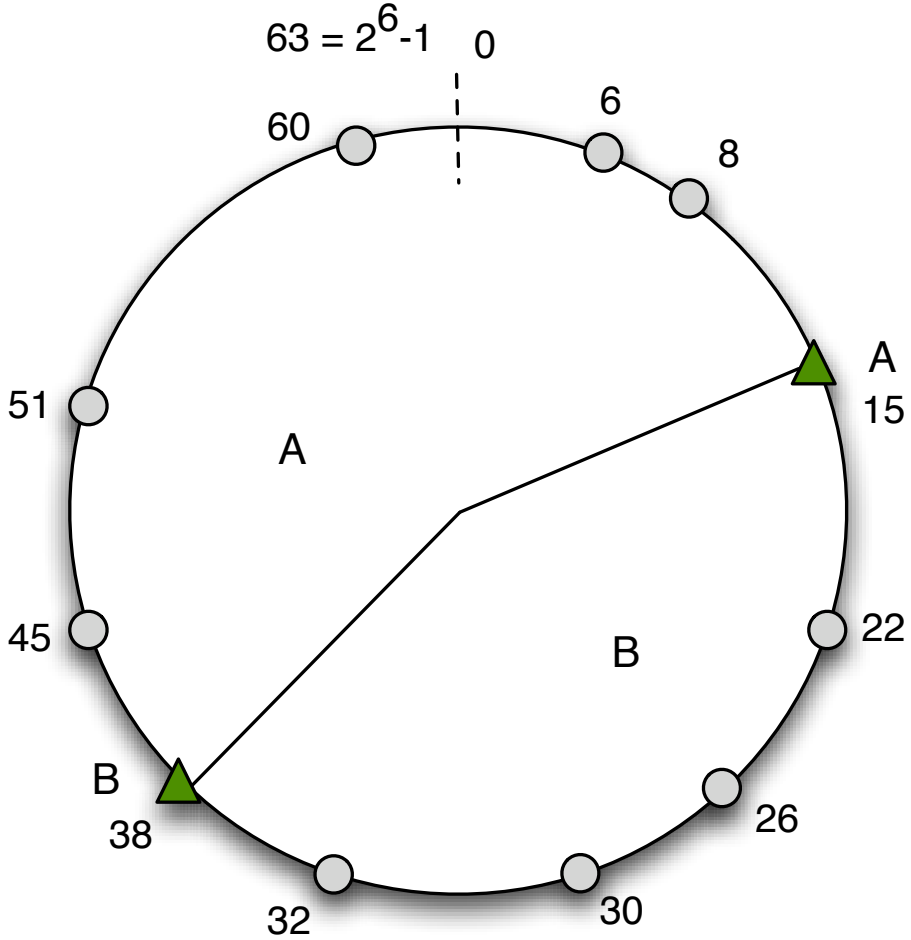
Exemple d'overlay structuré



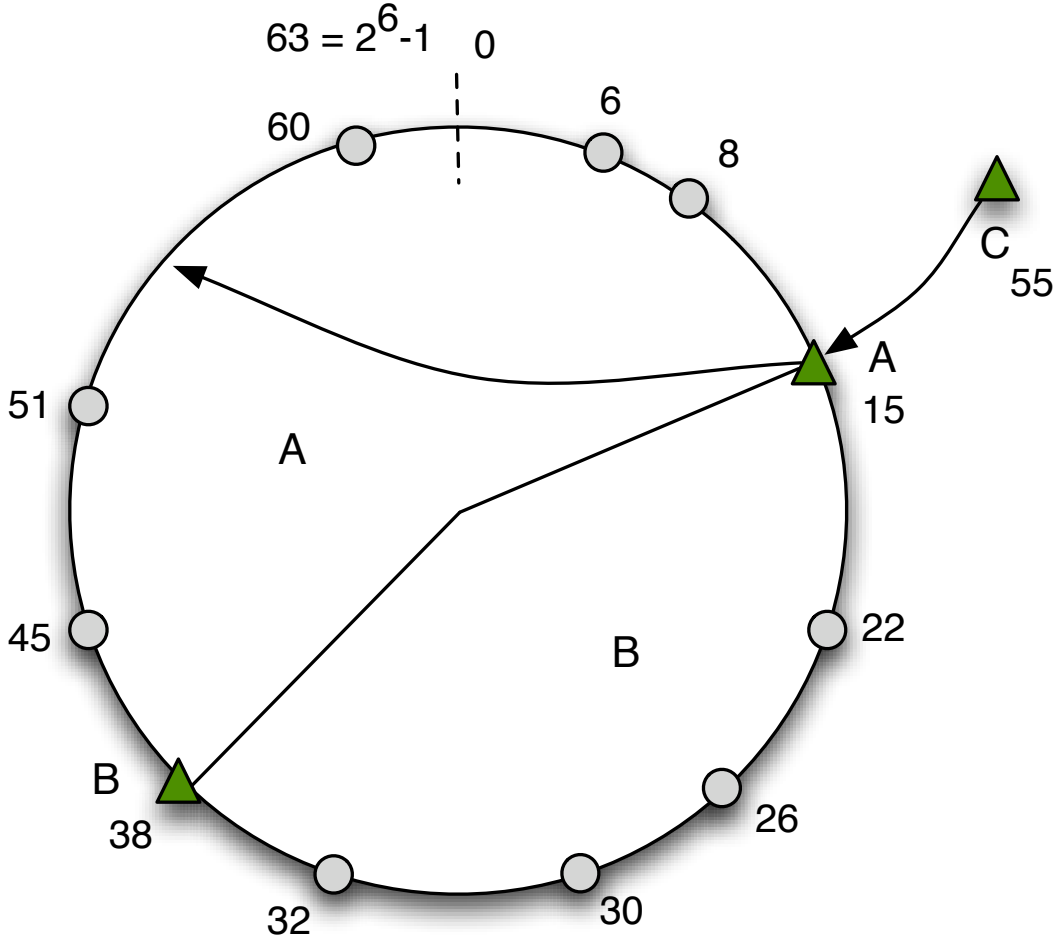
Exemple d'overlay structuré



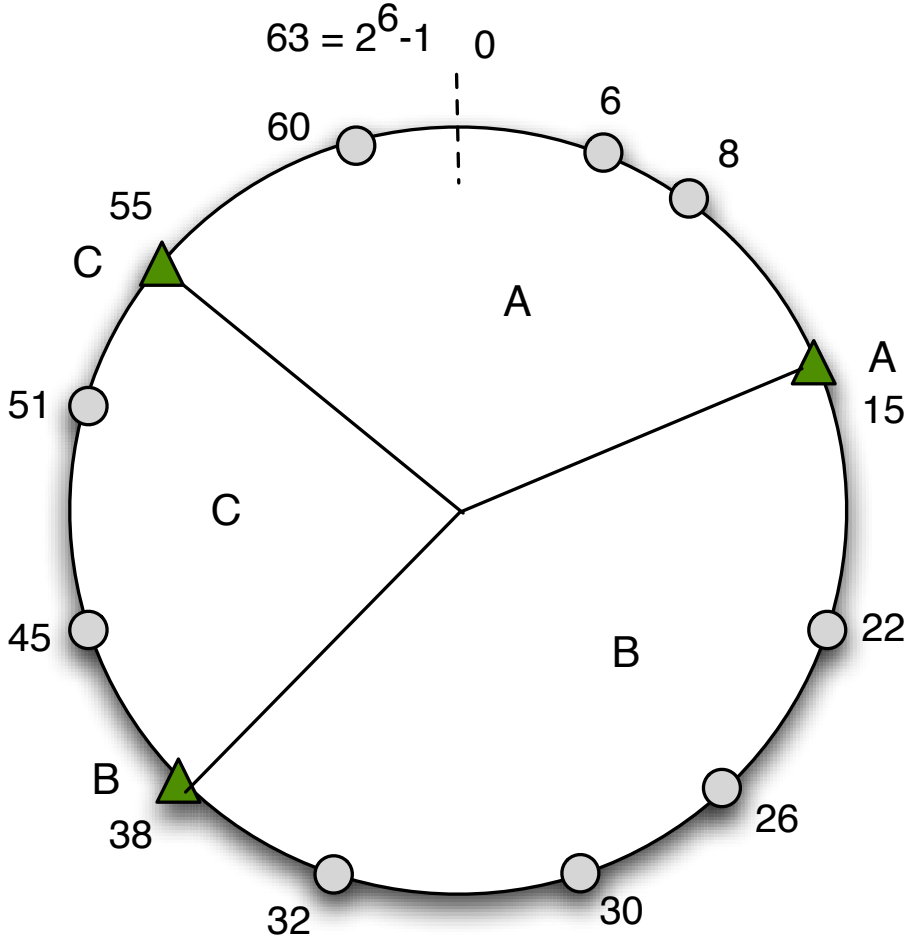
Exemple d'overlay structuré



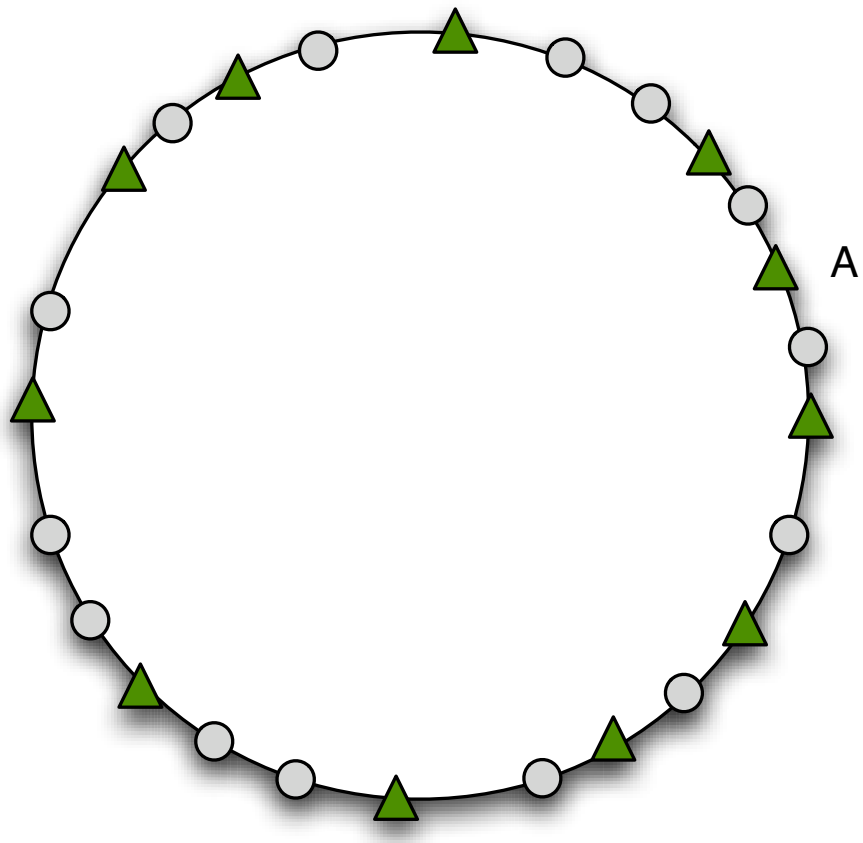
Exemple d'overlay structuré



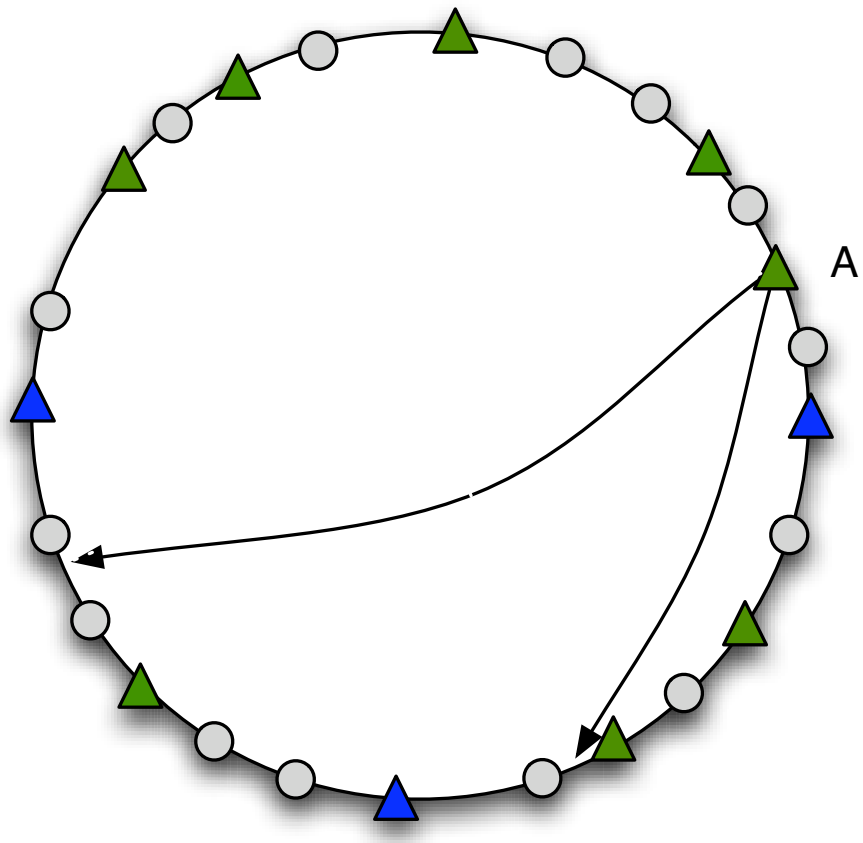
Exemple d'overlay structuré



Exemple d'overlay structuré



Exemple d'overlay structuré



Qu'est-ce que la Sybil Attack ?

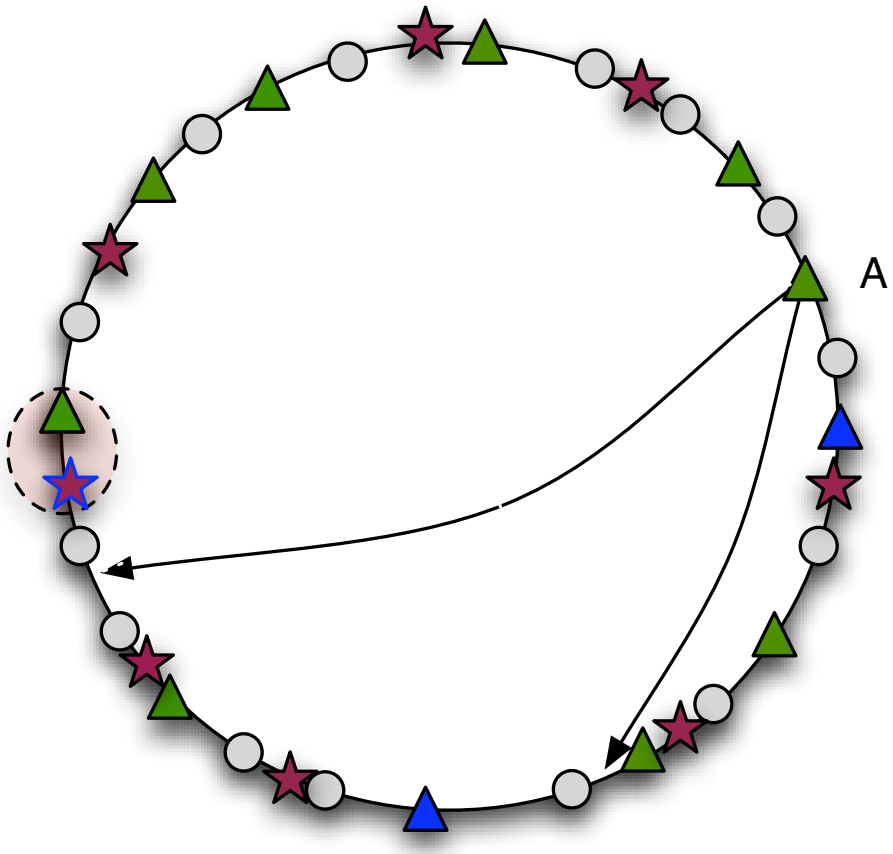
Réseau normal

1. Chaque utilisateur choisit aléatoirement un unique identifiant
2. Ces identifiants génèrent une distribution uniforme dans l'espace

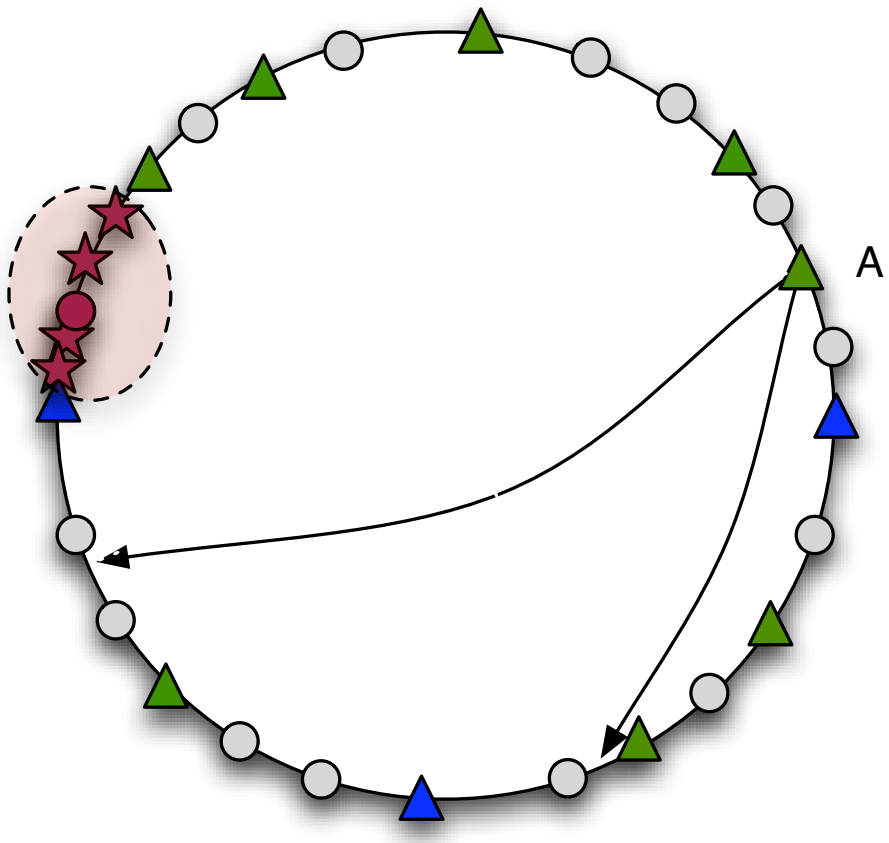
En cas de Sybil Attack

1. Un unique attaquant choisit n identifiants
2. Cet unique attaquant corrompt la distribution des identifiants dans l'espace

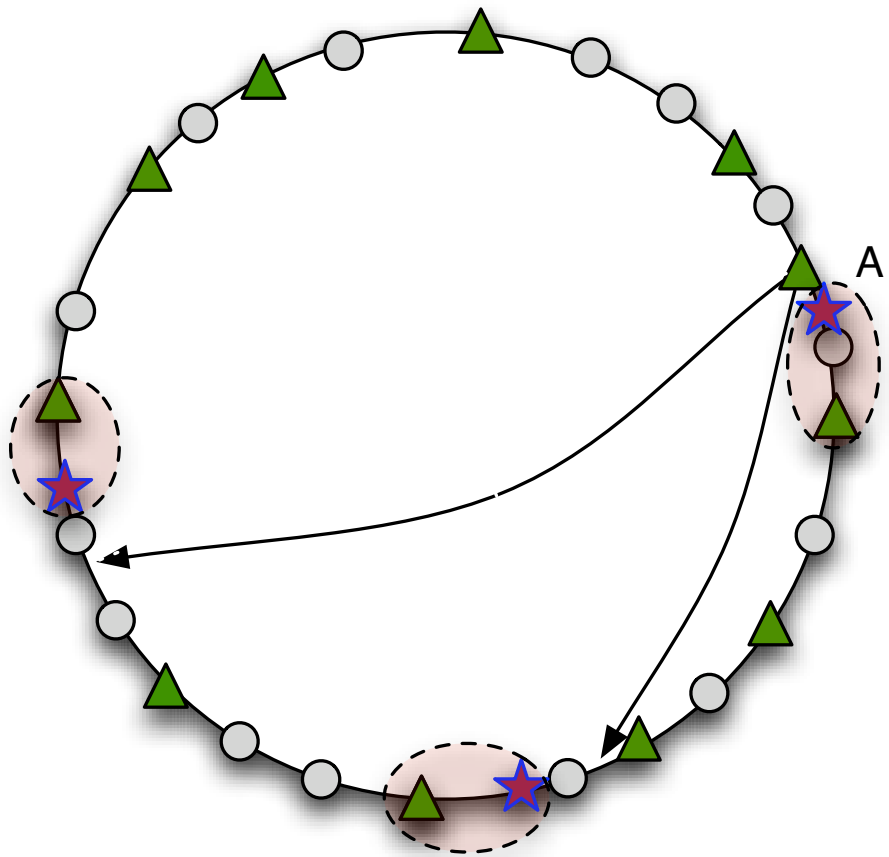
Attaque globale



Attaque d'une ressource



Attaque d'un nœud



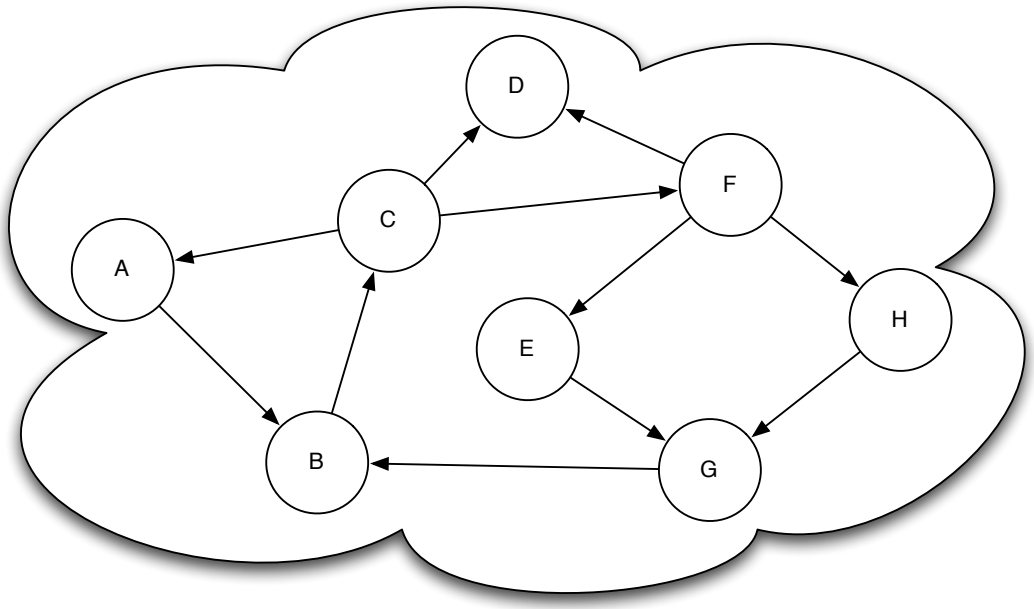
Objectifs pour limiter la Sybil Attack

Afin de limiter la Sybil Attack, il faut :

- Limiter le nombre d'identifiants d'une personne physique
- Contraindre ces identifiants à être choisis aléatoirement

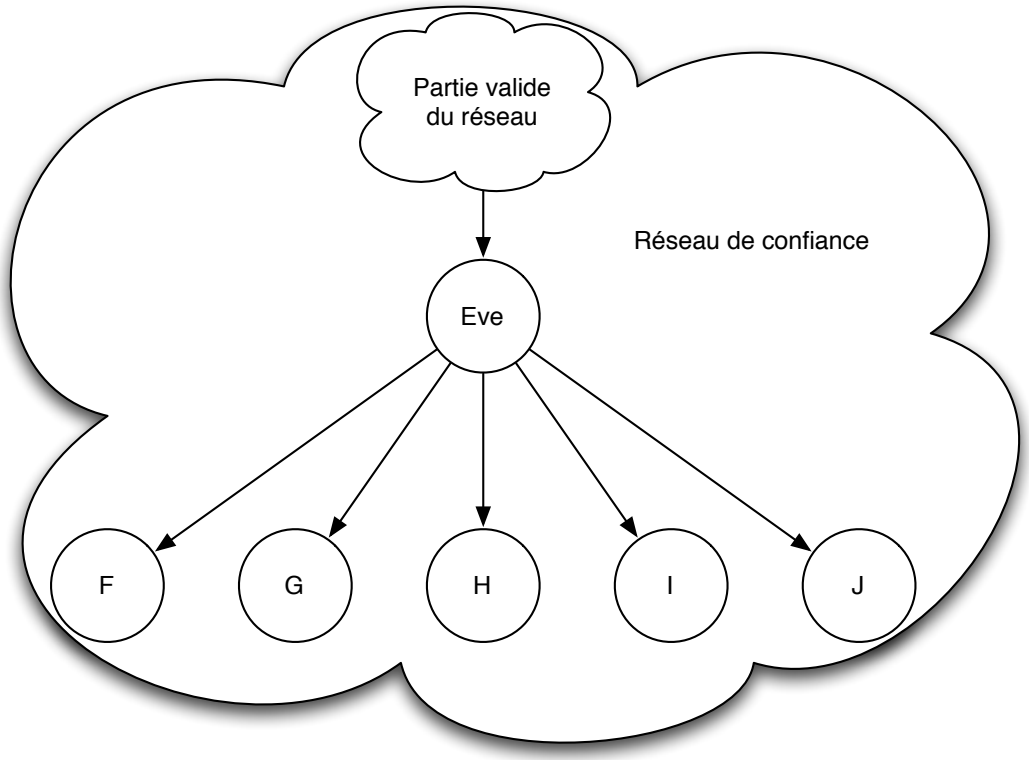
La limitation est obtenue par l'association d'un coût à un identifiant : monétaire, informatique, social...

Représentation des liens dans un graphe



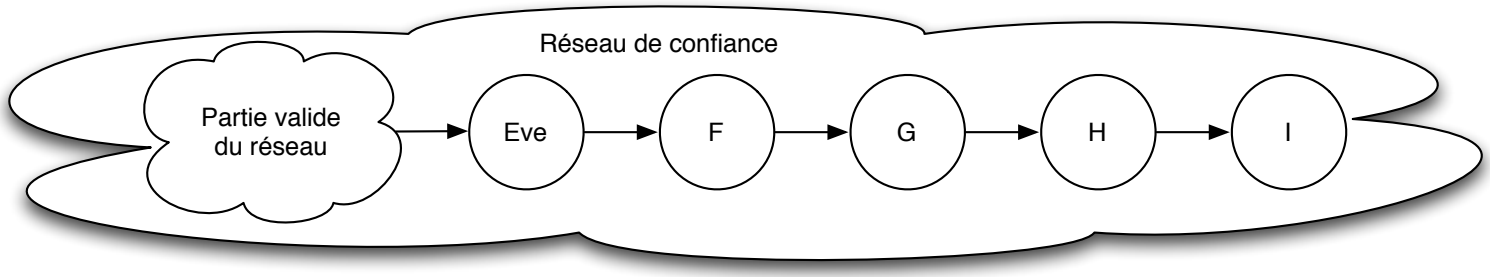
Graphe social (de confiance)

Attaque en largeur



Un attaquant crée un grand nombre d'identités directement
Limiter le degré sortant ?

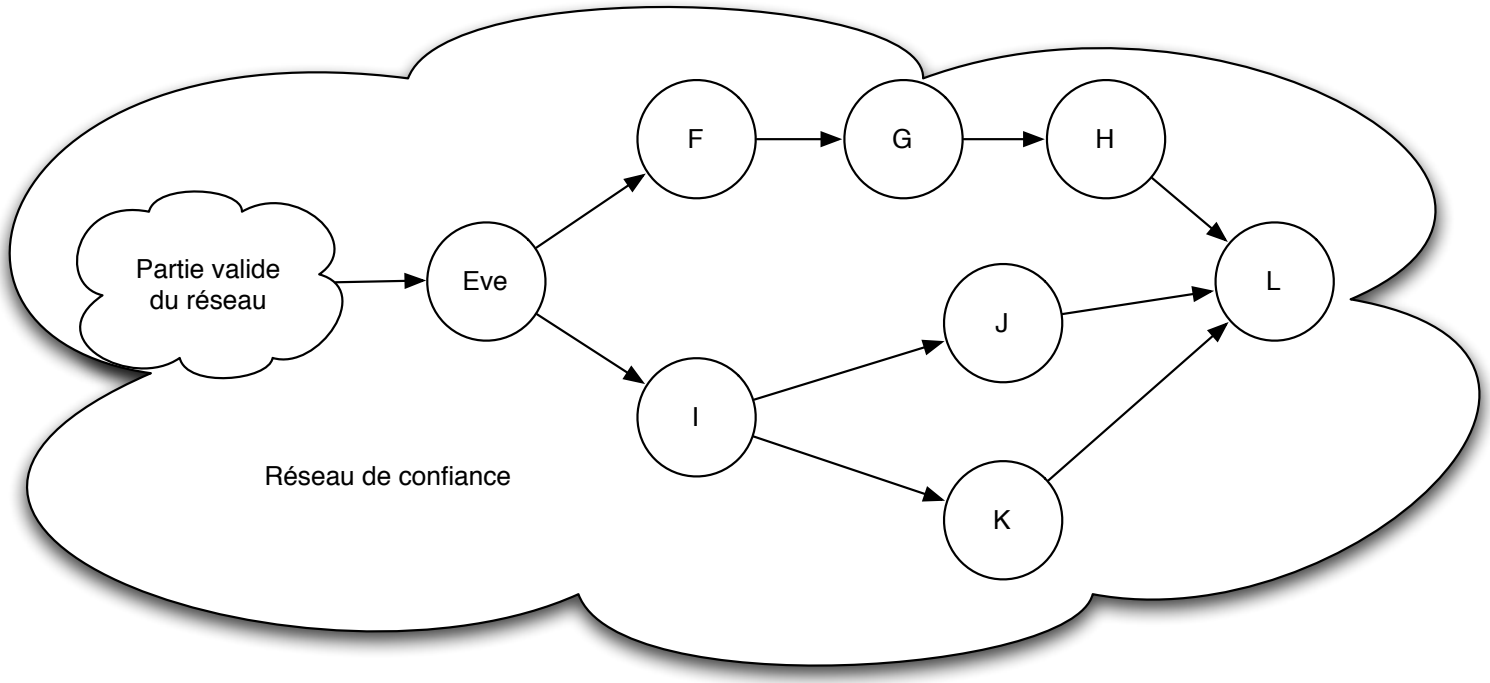
Attaque en longueur



Un attaquant crée une chaîne de fausses identités

Limiter la longueur des chaînes ?

Attaque mixte



Un attaquant crée un grand nombre d'identités
Limiter le poids sans connaître le graphe !

Point de départ

- Sybil attack ⇒ Beaucoup de fils dans le graphe
- Comment quantifier ce "beaucoup" ? ⇒ Comparaison aux autres membres
- Système à invitations : chaque membre possède un nombre d'invitations contraint par les autres membres

Représentation des membres

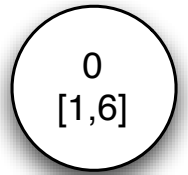
Les membres sont représentés dans un arbre :

- Cet arbre est créé par les membres fondateurs du réseau
- Les fils d'un nœud sont les membres invités par ce nœud
- La régulation des invitations contrôle les déséquilibres

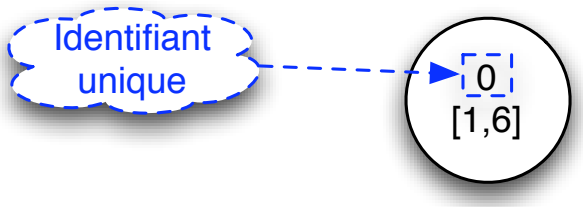
Cet arbre doit être :

- Suffisamment équilibré pour limiter une Sybil Attack
- Suffisamment souple pour insérer de nouveaux membres

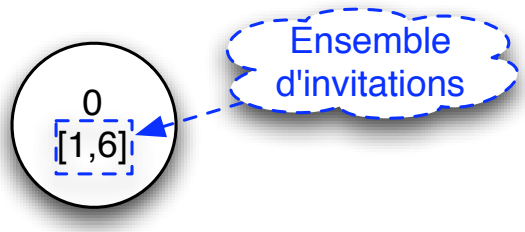
Nœuds de l'arbre des membres



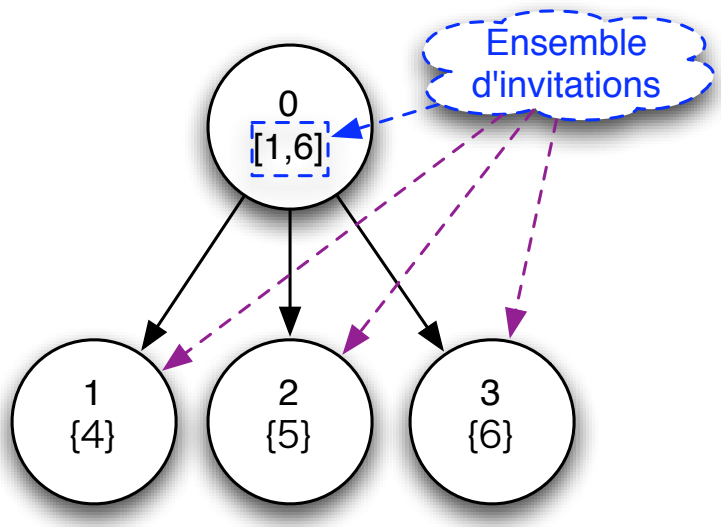
Nœuds de l'arbre des membres



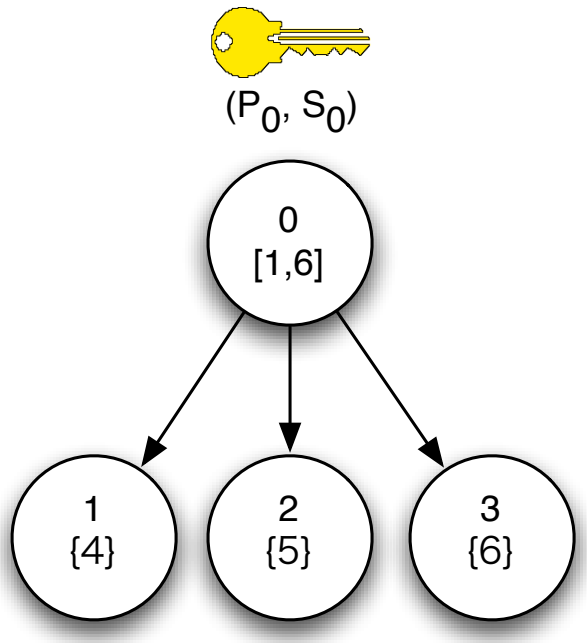
Nœuds de l'arbre des membres



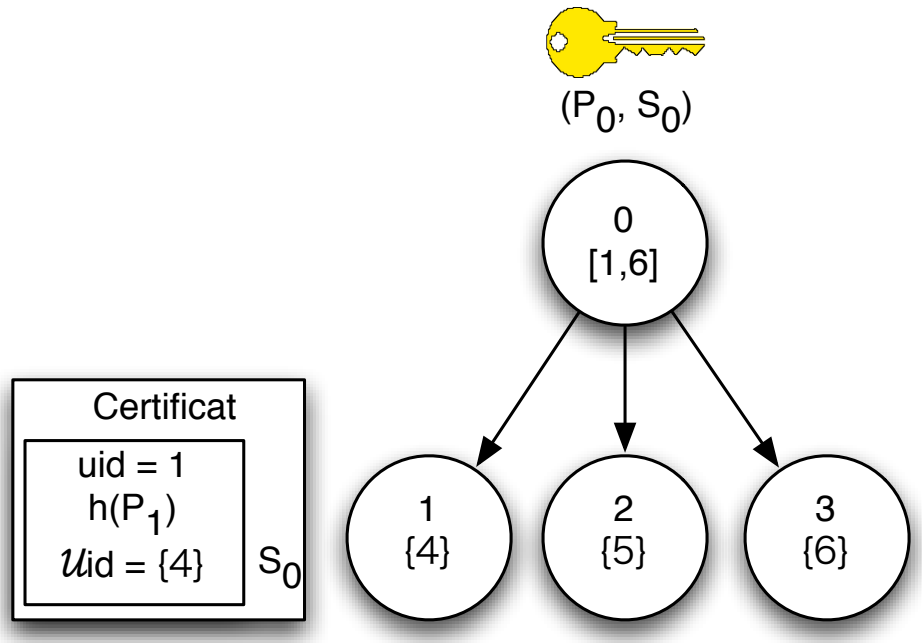
Nœuds de l'arbre des membres



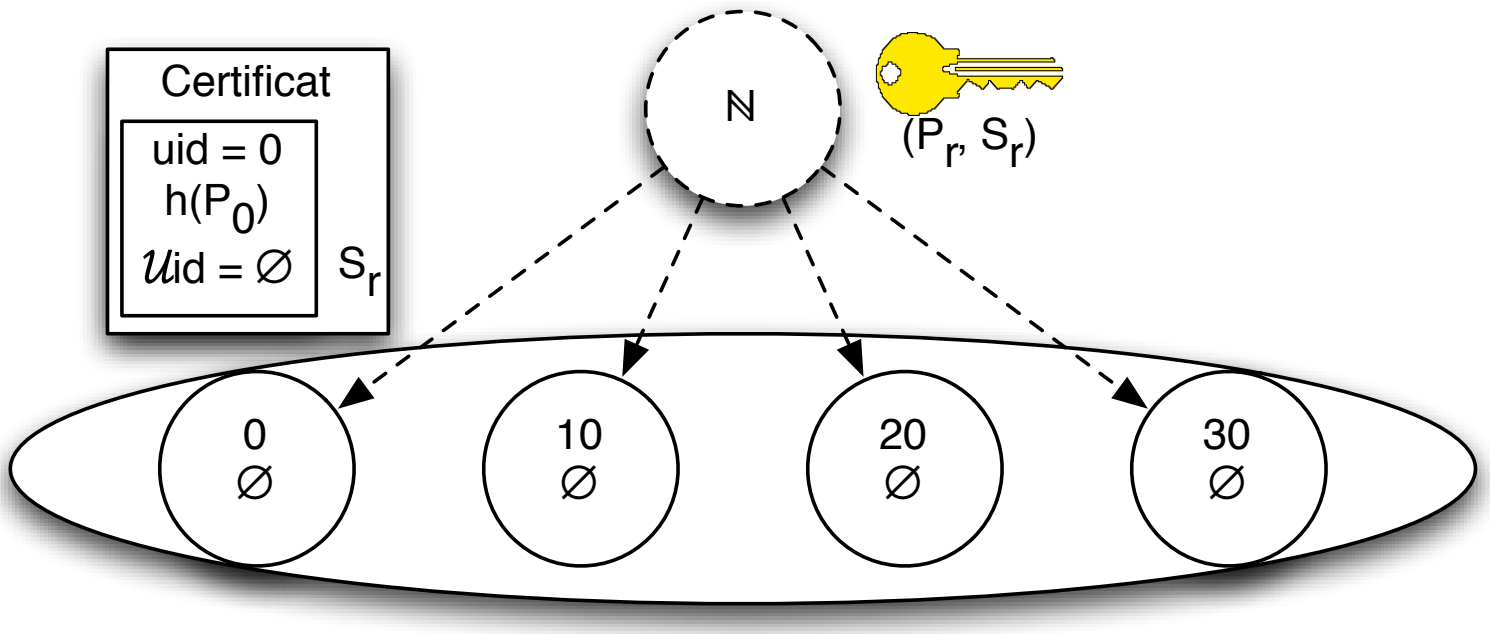
Nœuds de l'arbre des membres



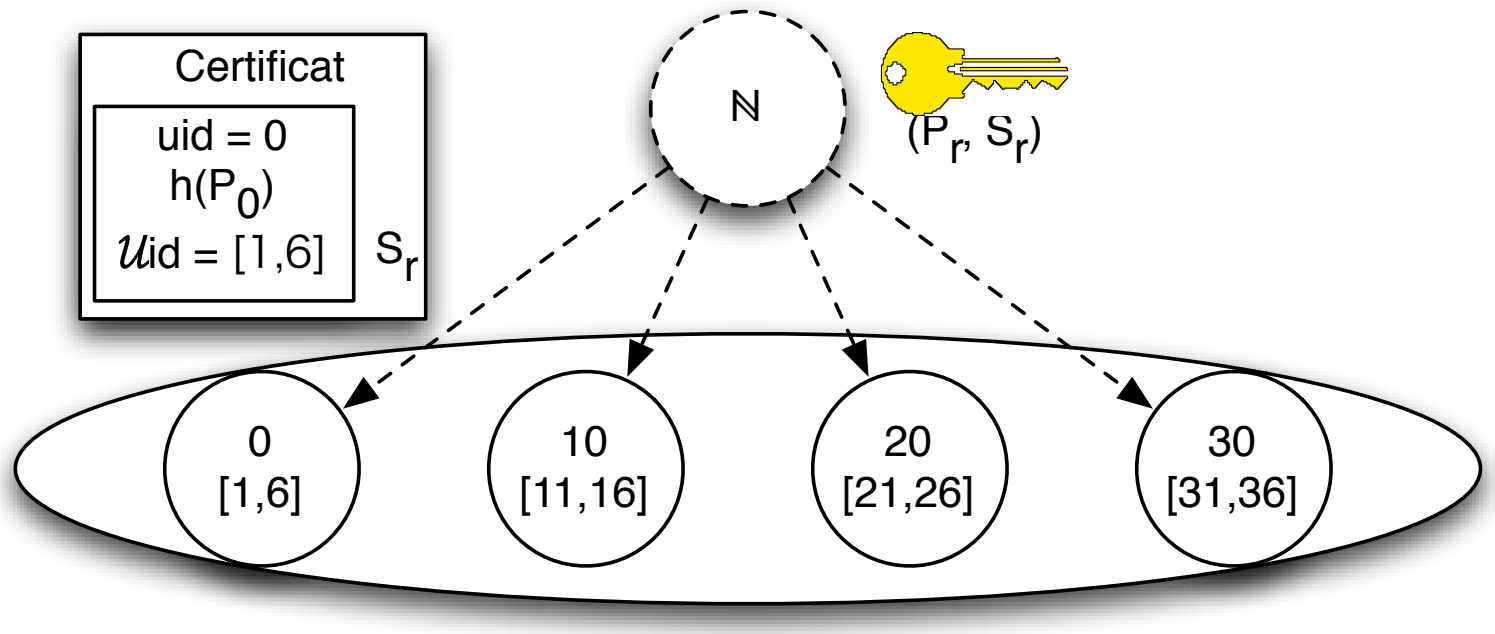
Nœuds de l'arbre des membres



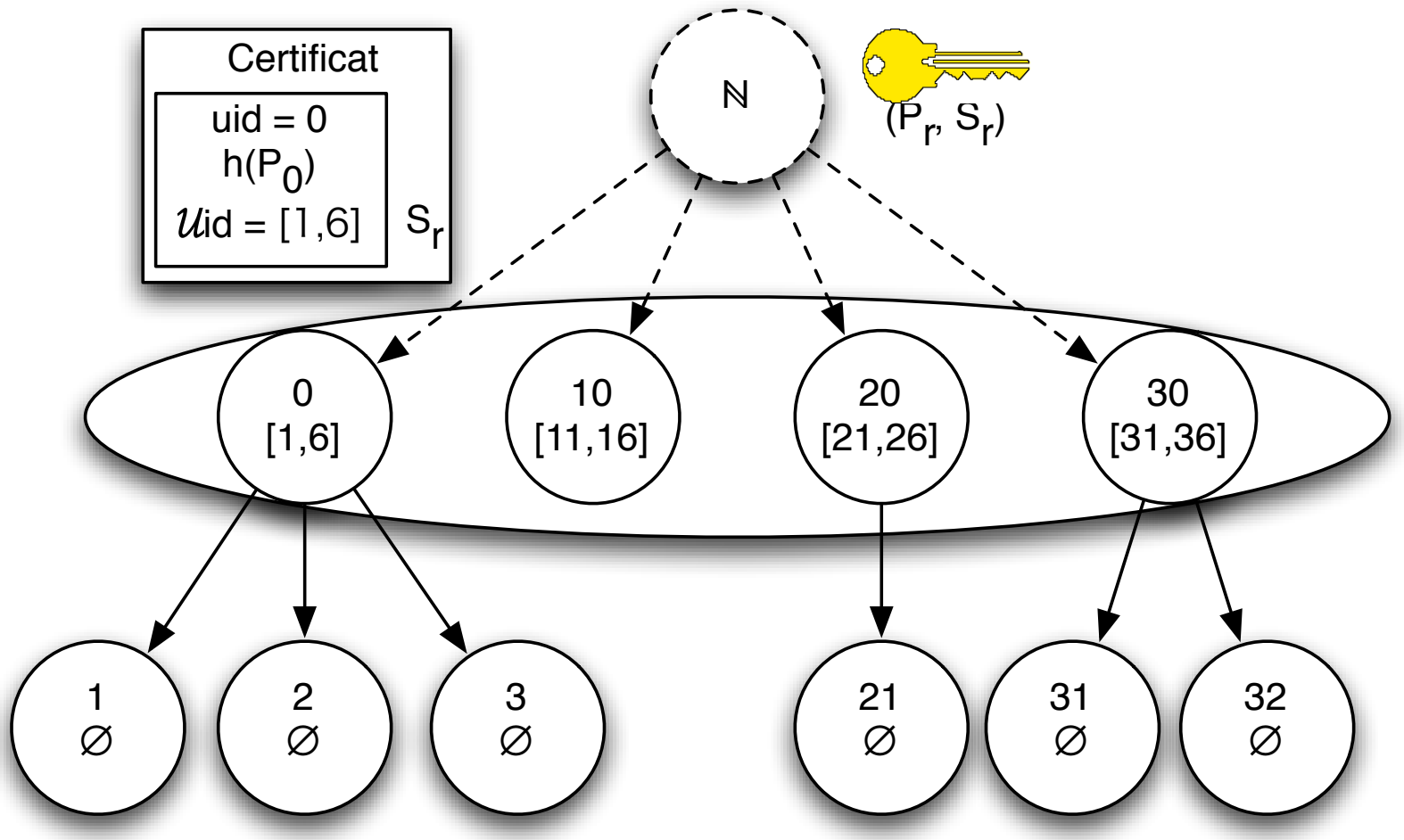
Création de l'arbre des membres



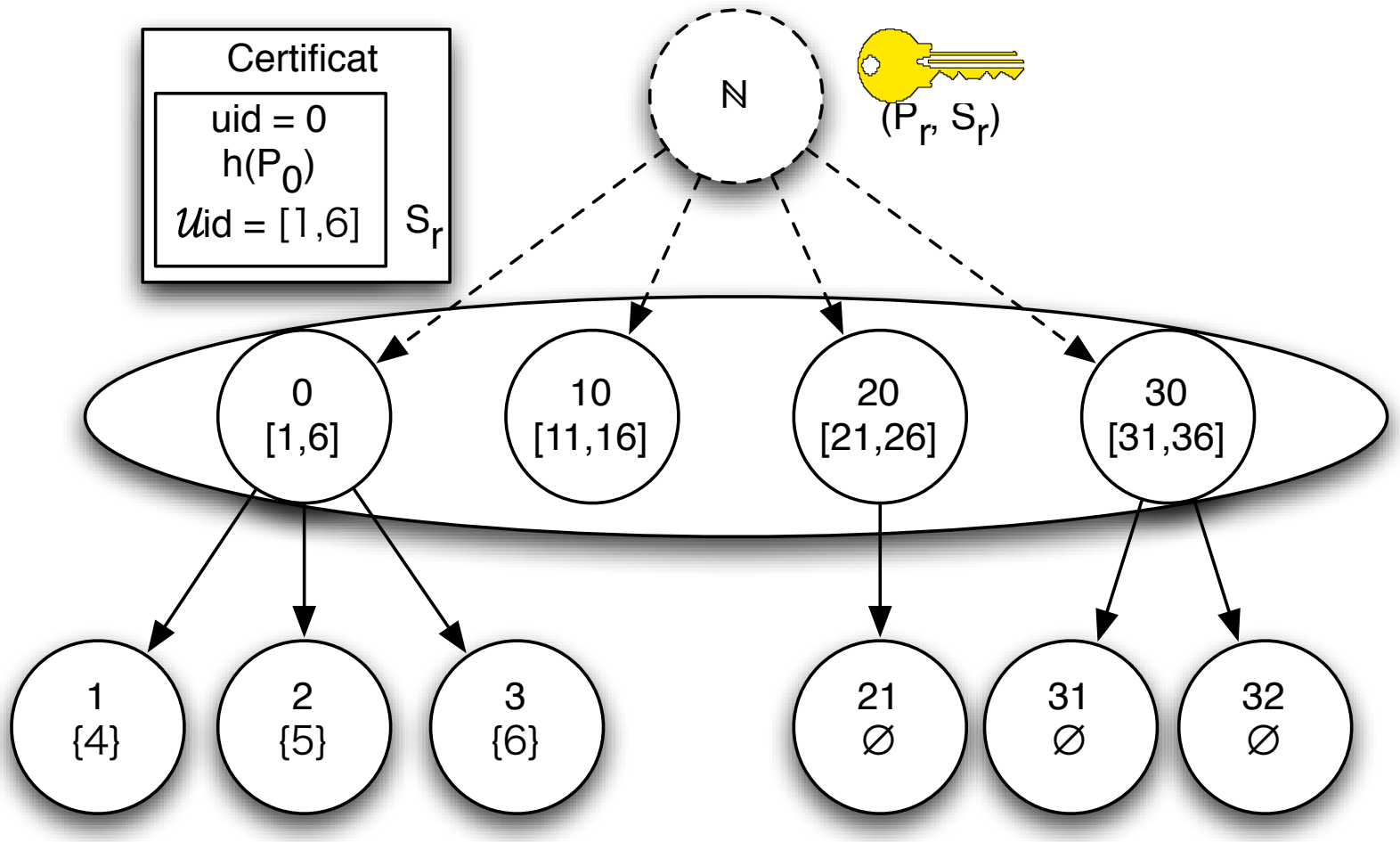
Création de l'arbre des membres



Création de l'arbre des membres



Création de l'arbre des membres



Politique de distribution

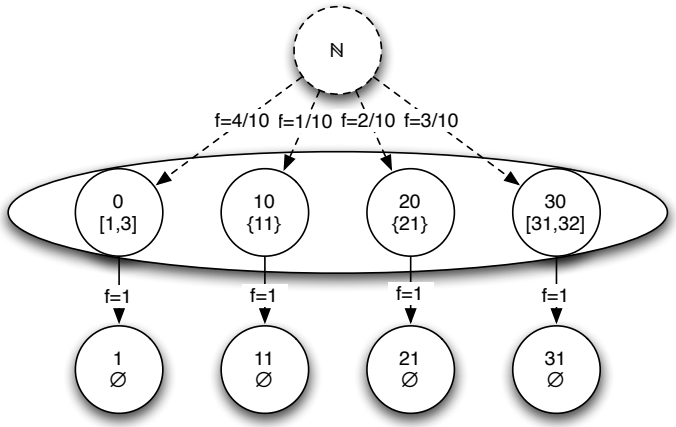
La distribution des invitations permet :

- Matérialisation des déséquilibres attendus : *facteur*
- Contrôle global des déséquilibres : contrôle local des invitations

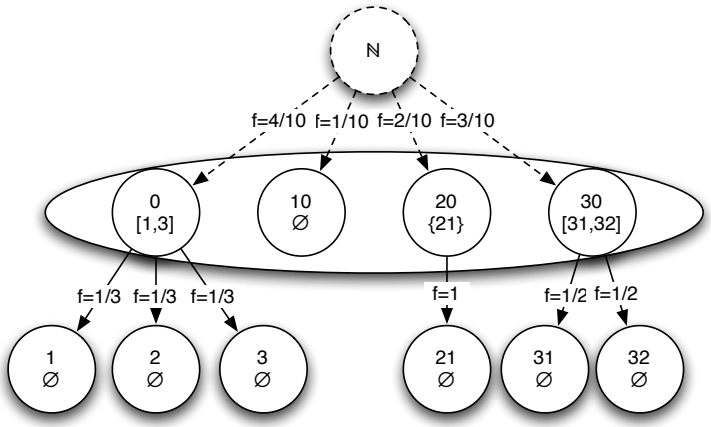
Un membre n'obtient d'invitations de son père que si son *poids* le permet

Remarque sur l'équilibre de l'arbre

L'arbre résultant n'est pas un arbre équilibré mais un arbre dont les déséquilibres sont contrôlés.



Arbre équilibré mais non contrôlé



Arbre déséquilibré mais contrôlé

Résistance à des personnes malveillantes

Le système proposé limite la Sybil Attack :

- Impossibilité de créer un grand nombre d'identités (limite des frères)
- Impossibilité de choisir son identifiant (choisi parmi les invitations du père)

Cependant, il convient de faire attention :

- Blocage par un attaquant (gestion du problème par le père)
- Rôle critique des membres fondateurs

Plus il y a d'étages de membres bienveillants en haut de l'arbre, plus les Sybil Attacks sont limitées.

Adaptation à des réseaux Pair-à-Pair

Dans le cadre des réseaux Pair-à-Pair :

- $NodeId = h(id)$ assure la diffusion des identifiants
- Les réseaux Pair-à-Pair croissent par recommandation sociale
  $\Rightarrow$ Tout le monde peut s'insérer

En contrepartie, un peu de centralisation nécessaire [*Cheng et al.*]

Gestion distribuée d'identités résistante à la Sybil Attack pour un réseau Pair-à-Pair

François Lesueur, Ludovic Mé, Valérie Viet Triem Tong

Supélec, équipe SSIR (EA 4039)

13 juin 2007