Objets physiques agrégés et sûreté de fonctionnement

Fabrice Ben Hamouda

Centre de recherche INRIA Rennes - Bretagne Atlantique
Équipe ACES (Ambient Computing and Embedded Systems)
Stage de 3 mois
Sous la direction de Michel Banâtre et Fabien Allard

Lundi 13 Septembre 2010

1. Introduction
   - Les objets physiques agrégés
   - Les objets agrégés en arbre
   - Réalisation pratique

2. Formats d'agrégation
   - Généralités
   - Troisième format arborescent
   - Sécurité et décodage unique

3. Sûreté de fonctionnement
   - Introduction
   - Sécurité des formats d'agrégation arborescents
   - Une solution à base de tags Alien
   - Performances

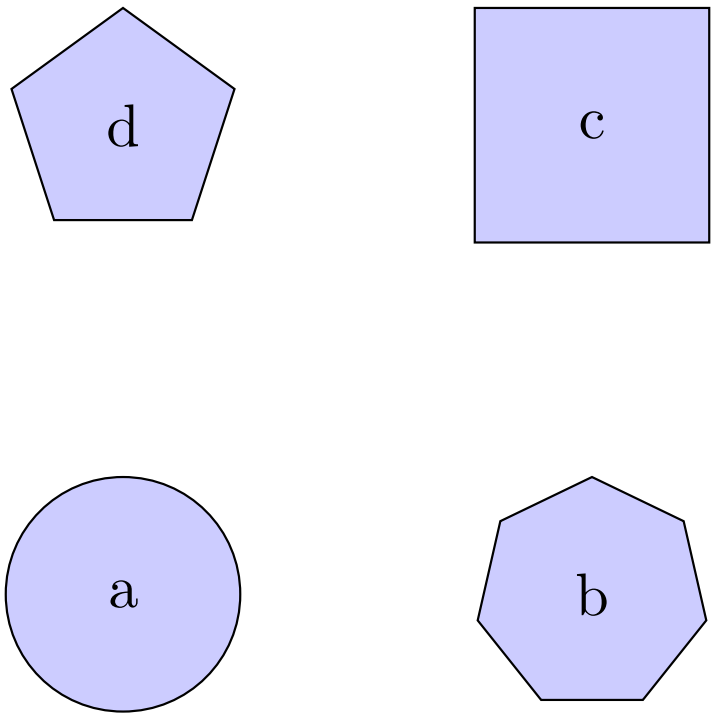
1. Introduction
   - Les objets physiques agrégés
   - Les objets agrégés en arbre
   - Réalisation pratique

2. Formats d'agrégation
   - Généralités
   - Troisième format arborescent
   - Sécurité et décodage unique

3. Sûreté de fonctionnement
   - Introduction
   - Sécurité des formats d'agrégation arborescents
   - Une solution à base de tags Alien
   - Performances

Les objets physiques agrégés

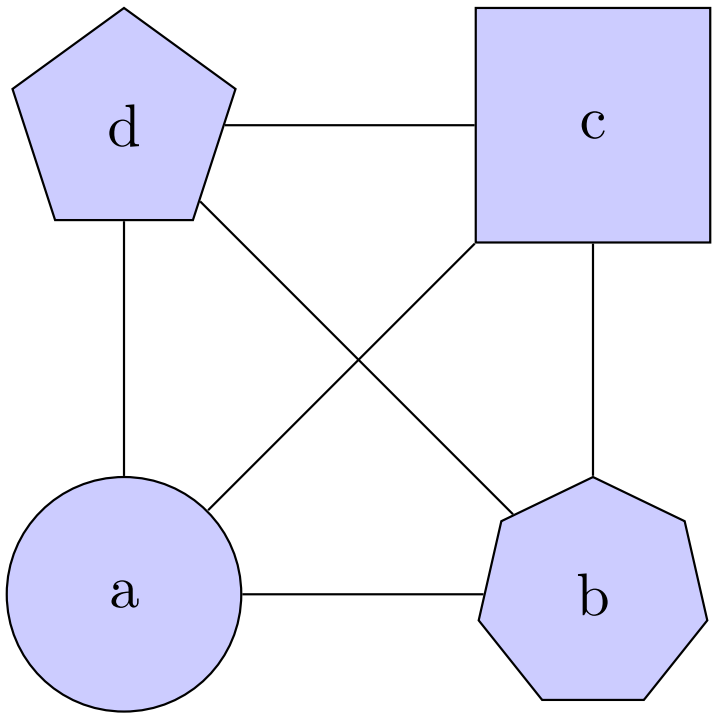
- **Objet physique agrégé (ou couplé)** : ensemble d'**objets physiques** mobiles et/ou physiquement indépendants (appelés **fragments**).
- Vérification de l'**intégrité** dans des **zones de contrôle** identifiées.



Fragments non agrégés

Les objets physiques agrégés

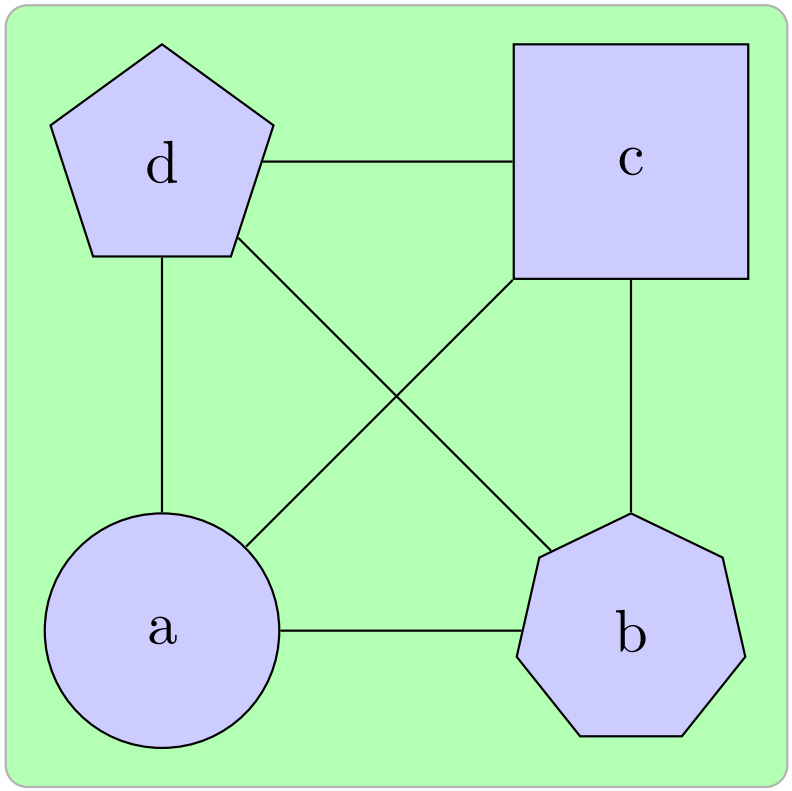
- **Objet physique agrégé (ou couplé)** : ensemble d'**objets physiques** mobiles et/ou physiquement indépendants (appelés **fragments**).
- Vérification de l'**intégrité** dans des **zones de contrôle** identifiées.



Objet agrégé

Les objets physiques agrégés

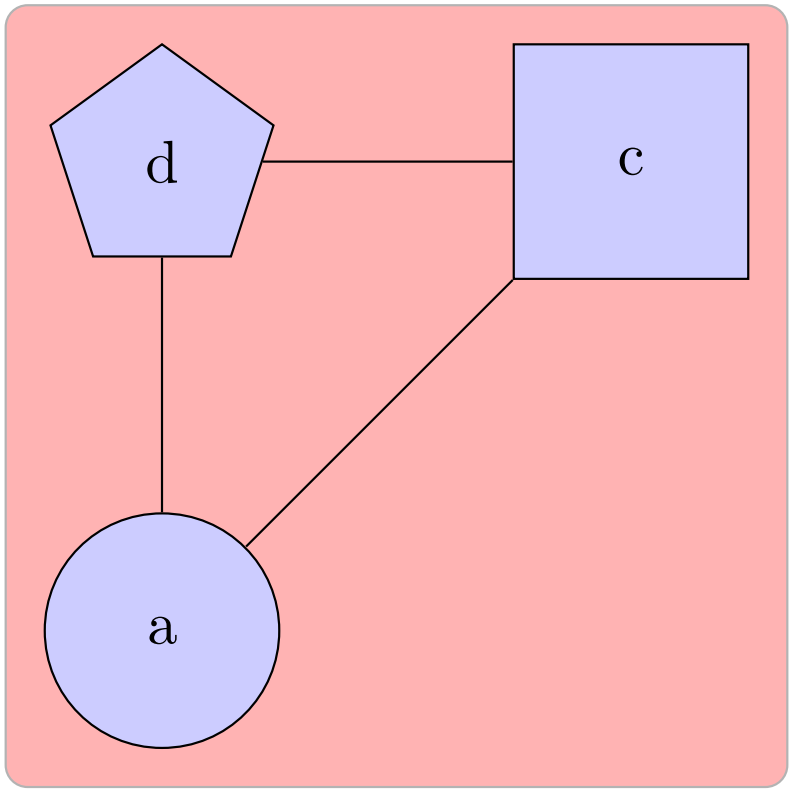
- **Objet physique agrégé (ou couplé)** : ensemble d'**objets physiques** mobiles et/ou physiquement indépendants (appelés **fragments**).
- Vérification de l'**intégrité** dans des **zones de contrôle** identifiées.



Objet agrégé intègre dans zone de contrôle

Les objets physiques agrégés

- **Objet physique agrégé (ou couplé)** : ensemble d'**objets physiques** mobiles et/ou physiquement indépendants (appelés **fragments**).
- Vérification de l'**intégrité** dans des **zones de contrôle** identifiées.



Partie d'un objet agrégé dans zone de contrôle

Analogie avec la transmission par paquets

Envoi d'un fichier F sur le réseau.

- Émetteur :
  - Découpage de F en paquets.
  - Envoi des paquets indépendamment sur le réseau de communication.
- Récepteur :
  - Réception des paquets de F.
  - Réassemblage des paquets pour obtenir F.
  - Vérification de l'**intégrité** du fichier reçu.

Analogie avec la transmission par paquets

Envoi d'un fichier F sur le réseau.

- Émetteur :
  - Découpage de F en paquets.
  - Envoi des paquets indépendamment sur le réseau de communication.
- Récepteur :
  - Réception des paquets de F.
  - Réassemblage des paquets pour obtenir F.
  - Vérification de l'**intégrité** du fichier reçu.

- Les **paquets** correspondent aux **fragments**.
- Le **fichier** correspond à l'**objet agrégé**.
- Les **zones de contrôle** sont le récepteur et les routeurs.

Analogie avec la transmission par paquets

Envoi d'un fichier F sur le réseau.

- Émetteur :
  - Découpage de F en paquets.
  - Envoi des paquets indépendamment sur le réseau de communication.
- Récepteur :
  - Réception des paquets de F.
  - Réassemblage des paquets pour obtenir F.
  - Vérification de l'**intégrité** du fichier reçu.

- Les **paquets** correspondent aux **fragments**.
- Le **fichier** correspond à l'**objet agrégé**.
- Les **zones de contrôle** sont le récepteur et les routeurs.

- Paquets entrelacés sur le réseau de communication.
- Informations nécessaires au réassemblage du fichier dans les paquets.

Les objets agrégés - UbiCheck

Exemple d'application : UbiCheck

Objectif : s'assurer que les voyageurs en avion n'égarent leurs bagages cabine ni ne prennent ceux des autres.

- À l'entrée de l'aéroport :
  création de l'objet agrégé « voyageur + porte-feuille + valises ».
- A l'entrée/sortie de l'avion, après les rayons X, . . . :
  l'intégrité de l'objet agrégé est vérifiée.

Les objets agrégés en arbre

Un **objet physique agrégé** peut lui-même contenir des objets agrégés.

Exemple

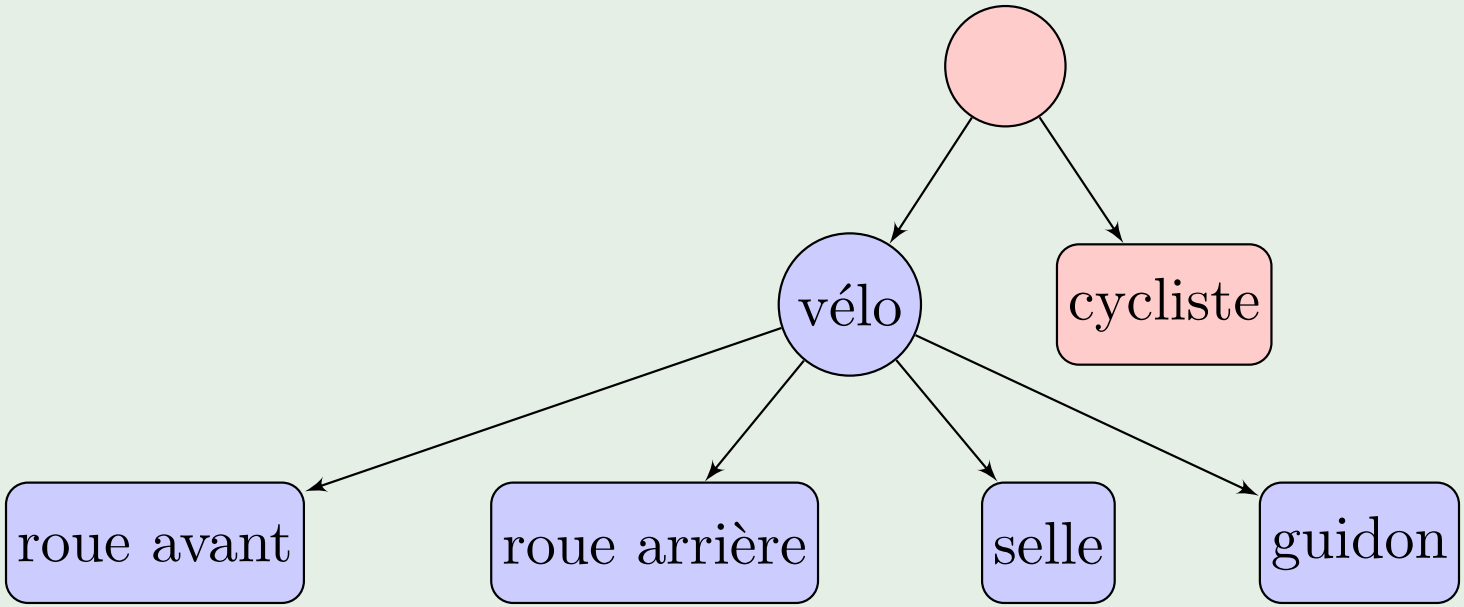


FIGURE : Un cycliste et son vélo (composé d'une selle, un guidon, ...)

Un tel objet agrégé peut servir de « clé » pour un local à vélos.

Les objets agrégés - réalisation pratique

L'information des objets couplés est stockée sur les fragments. Pour cela, les fragments sont équipés d'un tag RFID (Radio Frequency IDentification).

Les tags RFID :

- Petits dispositifs électroniques contenant une puce et une antenne.
- **Étiquette adhésive**, **badge** ou **intégrés aux objets** (cadre de vélo, pneus).
- Lecture/écriture par des **lecteurs RFID**.
- **Identifiant** (**id**) en lecture seule et **mémoire utilisateur** en lecture/écriture.

FIGURE : Étiquette RFID Alien (95mm x 8.2mm)

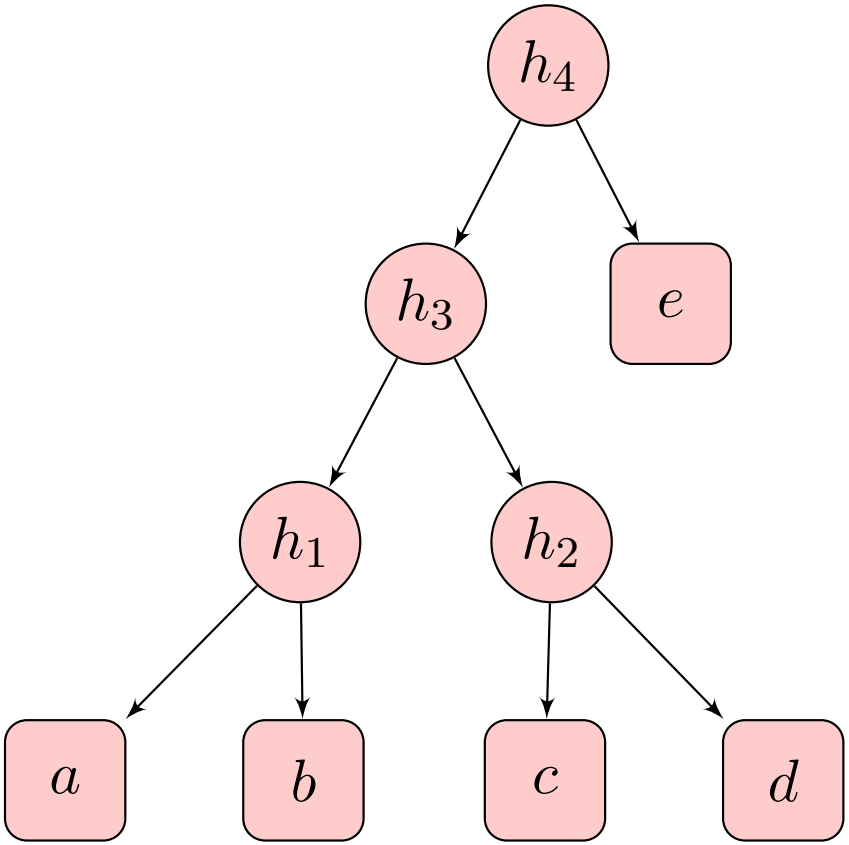
1 Introduction
- Les objets physiques agrégés
- Les objets agrégés en arbre
- Réalisation pratique

2 Formats d'agrégation
- Généralités
- Troisième format arborescent
- Sécurité et décodage unique

3 Sûreté de fonctionnement
- Introduction
- Sécurité des formats d'agrégation arborescents
- Une solution à base de tags Alien
- Performances

Format d'agrégation

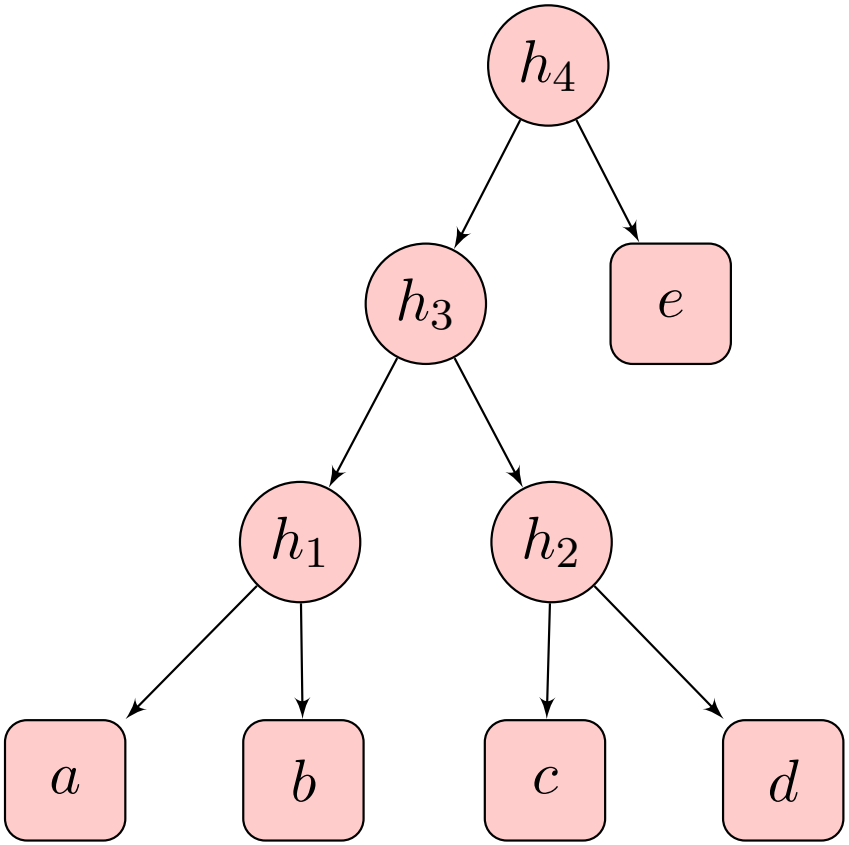
Objectif : trouver un moyen de représenter les objet agrégés.



- Feuilles : fragments (avec tag RFID) de valeur l'id du tag.

Format d'agrégation

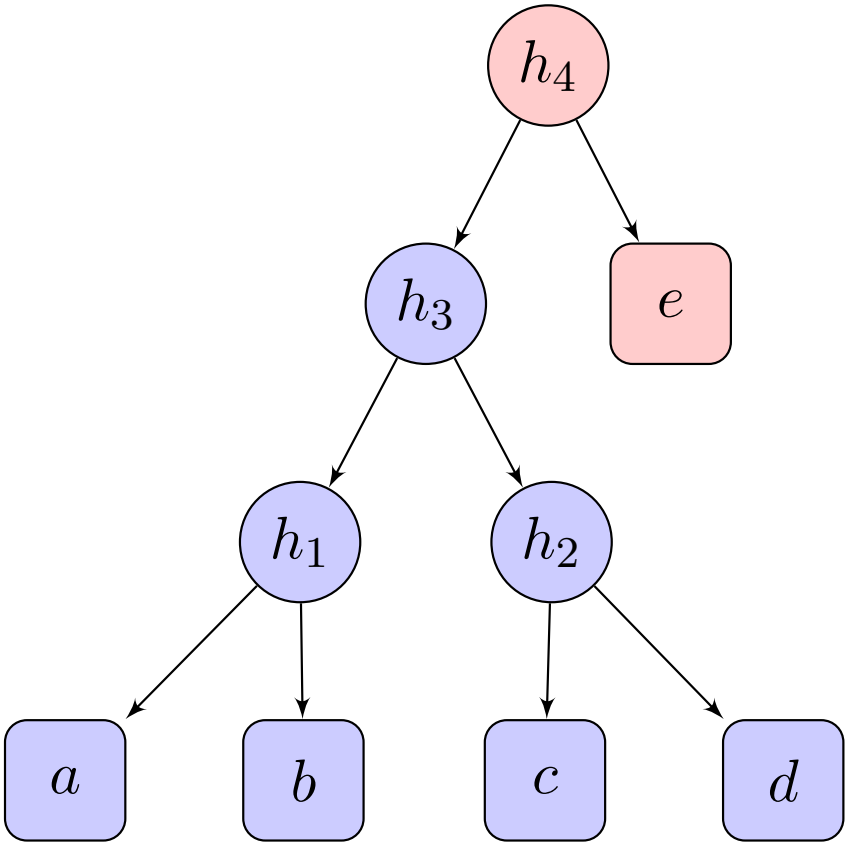
Objectif : trouver un moyen de représenter les objet agrégés.



- Feuilles : fragments (avec tag RFID) de valeur l'id du tag.
- Nœuds : sans mémoire — correspondent aux objets agrégés.

Format d'agrégation

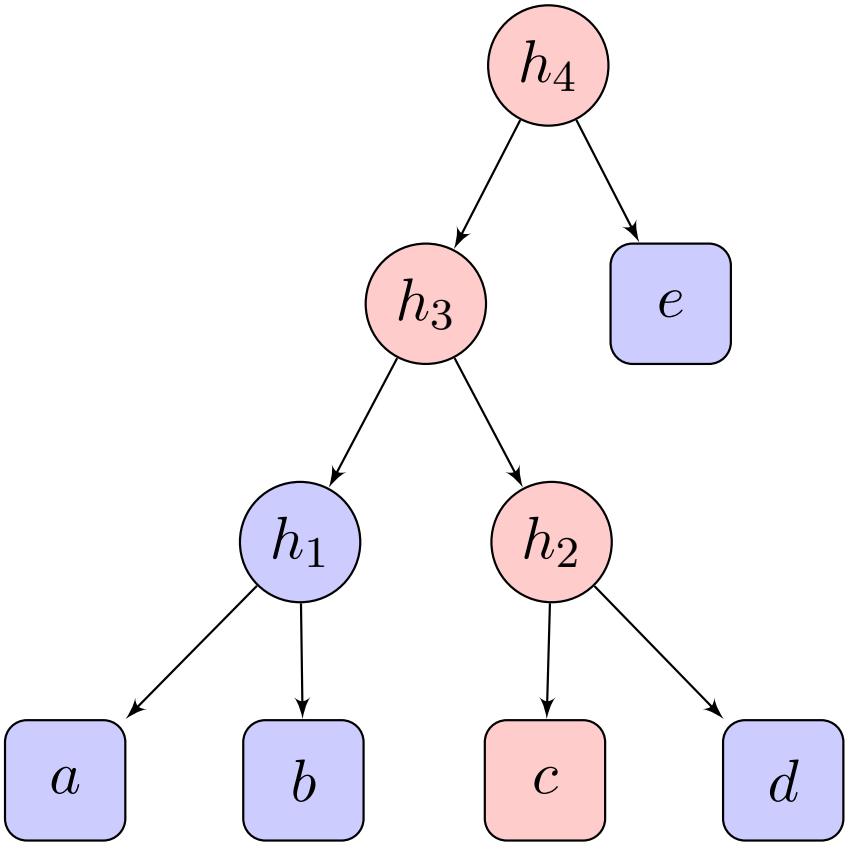
Objectif : trouver un moyen de représenter les objet agrégés.



Objectif : être capable de déterminer les sous-arbres maximaux contenant des tags donnés.

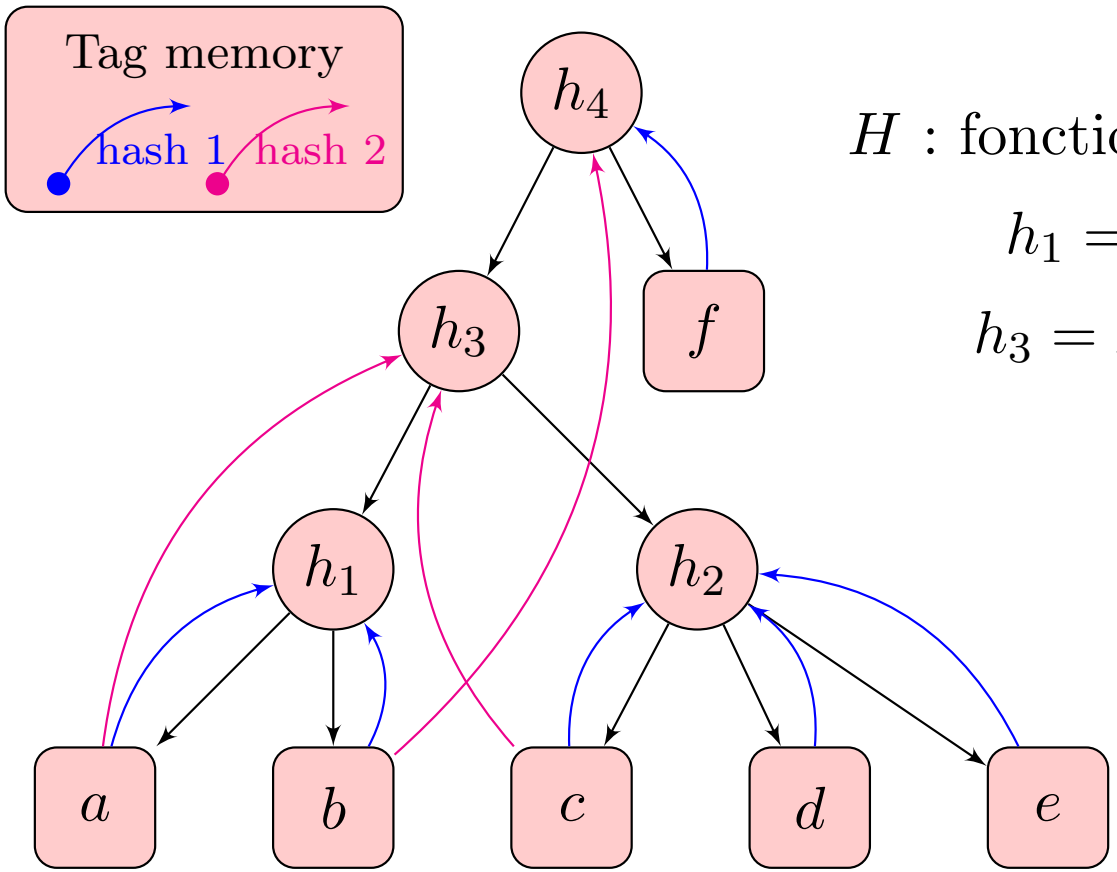
Format d'agrégation

Objectif : trouver un moyen de représenter les objet agrégés.



Objectif : être capable de déterminer les sous-arbres maximaux contenant des tags donnés.

Troisième format arborescent



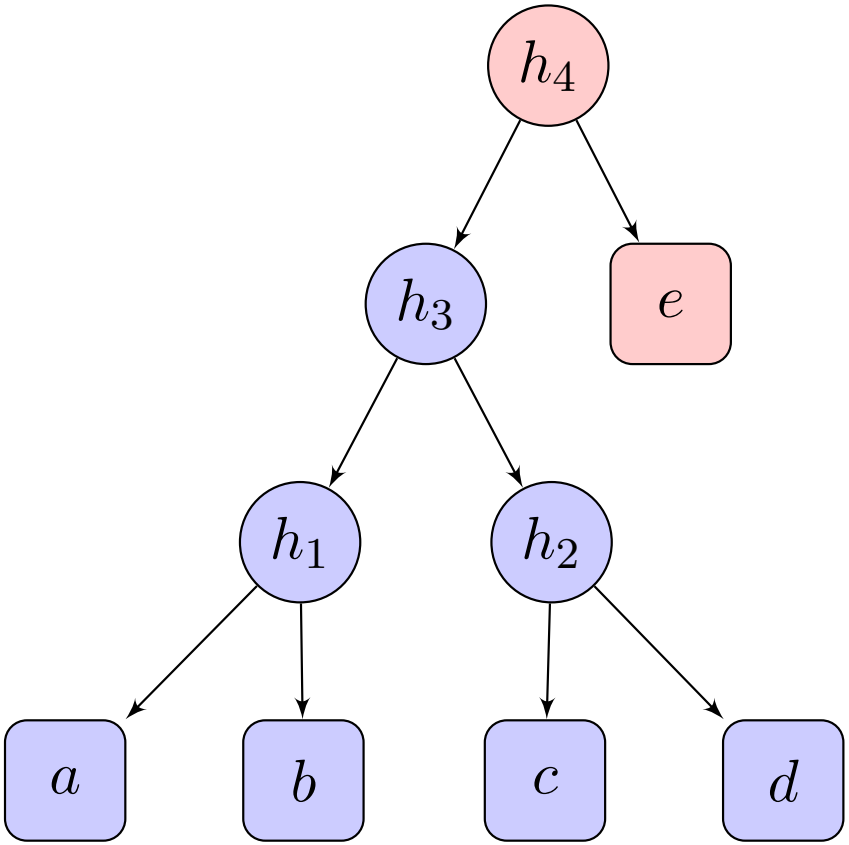
H : fonction de hachage

$$h_1 = H(a|b)$$

$$h_3 = H(h_1|h_2)$$

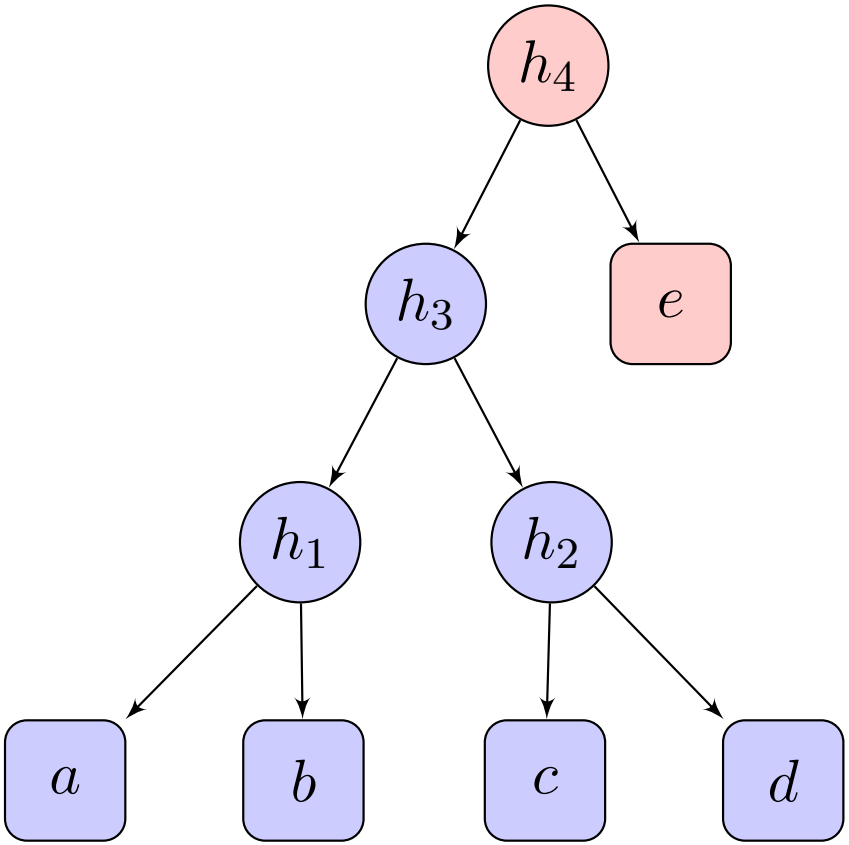
- Chaque tag contient deux zones mémoires (hashs 1 et 2 — magenta et bleu) contenant un id.
- À chaque fois, la zone mémoire libre la plus à gauche est choisie.

Sécurité et décodage unique



Intuitivement, si la fonction de hachage est bien choisie, l'id d'un nœud u définit le sous-arbre de racine u. D'où l'**unicité du décodage** dans toutes les solutions proposées.

Sécurité et décodage unique



Intuitivement, si la fonction de hachage est bien choisie, l'id d'un nœud u définit le sous-arbre de racine u. D'où l'**unicité du décodage** dans toutes les solutions proposées.

Mais cela ne garantit ni la **sécurité** ni un décodage **efficace**.

1. Introduction
   - Les objets physiques agrégés
   - Les objets agrégés en arbre
   - Réalisation pratique

2. Formats d'agrégation
   - Généralités
   - Troisième format arborescent
   - Sécurité et décodage unique

3. Sûreté de fonctionnement
   - Introduction
   - Sécurité des formats d'agrégation arborescents
   - Une solution à base de tags Alien
   - Performances

Sûreté de fonctionnement - introduction

Les objets agrégés ont été conçus pour faire de la sécurité, et notamment éviter :

- Substitution (par exemple de bagages), vols et attentats
- Utilisation non autorisée d'un service

Sûreté de fonctionnement - introduction

Les objets agrégés ont été conçus pour faire de la sécurité, et notamment éviter :

- Substitution (par exemple de bagages), vols et attentats
- Utilisation non autorisée d'un service

Ce sont les deux principales défaillances (des systèmes fondés sur les objets agrégés) à éviter — voir J.C. Laprie, *Dependability : basic concepts and terminology*.

Mais il y a d'autres défaillances possibles :

- Problèmes de disponibilité
- Violation de la vie privée

Sûreté de fonctionnement - fautes

- Fautes mécaniques, matérielles ou logicielles (non intentionnelles)
  - Porte cassée
  - Lecteur non fonctionnel

Sûreté de fonctionnement - fautes

- Fautes mécaniques, matérielles ou logicielles (non intentionnelles)
  - Porte cassée
  - Lecteur non fonctionnel
- Fautes humaines (externes intentionnelles)
  - Attaques physiques
    - Destruction de tags
    - Déplacement d'un tag
  - Attaques RF
    - Clonage de tags
    - Création/modification d'un objet agrégé (sans clonage)
    - Création de faux tags avec données aléatoires
    - Écriture de données aléatoires dans un vrai tag

Sécurité des formats d'agrégation arborescents

En supposant que la fonction de hachage est résistante au calcul d'une seconde préimage, il est **difficile de modifier** un objet agrégé en lecture seule.

Plus précisément :

Proposition

Les objets agrégés avec le troisième format arborescent vérifient les propriétés suivantes :

1. *l'**ajout** d'un tag ou d'un sous-arbre à un objet agrégé en lecture seule est difficile.*
2. *le **remplacement** d'un tag par un autre tag ou un sous-arbre (avec un **id différent**) dans un objet agrégé en lecture seule est difficile.*
3. *le **remplacement** d'un tag par un autre tag ou un sous-arbre dans un objet agrégé en lecture seule est difficile, si les tags ont un **id unique**.*

Implémentation - Tags Alien Higgs 3

Fonctionnalités des tags Alien :

- mémoire R/W : 512 + 96 bits
- verrou lecture/écriture : des zones mémoires peuvent être :
  - interdites d'écriture de façon permanente
  - protégées (à l'écriture ou à la lecture) par un mot de passe
- mémoire programmée en usine :
  96 bits dont 64 bits **UID** (Unique Id)
- authentification dynamique : assure l'authenticité du tag

FIGURE : Étiquette RFID Alien (95mm x 8.2mm)

Implémentation

Caractéristiques :

- Utilisation d'un **HMAC**-SHA-1-80 à la place d'une fonction de hachage
- **Signature** du tag avec DSA ou ECDSA
- **Chiffrement** du tag avec AES-CFB

De plus, les tags sont **interdits en écriture** :

- ou bien de façon permanente
- ou bien par un mot de passe

Implémentation – Organisation mémoire

512 bits répartis en :

Performances

- Nombre de tags lus par secondes :

  5 à 50 tags par seconde (selon les lecteurs)

- Cryptographie symétrique (AES-CFB, HMAC-SHA-1) :

  < 0.15 ms même sur mini-PC

- Cryptographie asymétrique (vérification de signature DSA (1024,320)) :

	Pentium M 2.0 GHz	Via Eden 500 MHz
Java + BC	12.8 ± 0.3 ms	136.7 ± 0.6 ms
Java + PadLock	n/a	9.5 ± 2.7 ms
OpenSSL	1.7 ms	12 ms

Conclusion - bilan

- Format d'agrégation
  - Un principe général pour les formats arborescents
  - Trois formats arborescents
  - Une extension : les CMPT
- Sûreté de fonctionnement
  - Analyse des attaques
  - Propositions théoriques
  - Analyse des tags existants et propositions pratiques
  - Benchmarks des primitives cryptographiques utilisées
- Implémentation (Java)
  - Deuxième format arborescent
  - Lecteur RFID virtuel
- Autres
  - Proposition (avec Jean-François, stagiaire des Mines de Nantes) d'une architecture globale pour les systèmes utilisant des objets agrégés
  - Signatures courtes et couplages sur les courbes elliptiques

Conclusion - problèmes ouverts

- D'un point de vue théorique :
  - Analyse de la sécurité de l'authentification dynamique des tags Alien (si accès aux documents)
  - Analyse plus précise de la sûreté de fonctionnement, notamment des erreurs et fautes mécaniques, matérielles ou logicielles, ...
  - Généralisation des formats d'agrégation

- D'un point de vue pratique :
  - Implémentation (en Java) de la nouvelle architecture
  - Tests précis des tags Alien / du lecteur Alien (notamment zones d'ombre, vitesse de lecture, tags décollables ou non, ...)
  - Analyse de la faisabilité d'attaques par canaux auxiliaires

Questions

Merci de votre attention