

Is My Password Safe ?

Une Introduction aux fonctions de condensats

Loïc Rouquette ¹

2025-01-23

¹LRE, Epita Research Laboratory

Table des matières

Qu'est ce que c'est ?	3
À quoi ça sert ?	4
Condensats Cryptographiques	7

Qu'est ce que c'est ?

Une fonction de condensation (ou fonction de hachage) est une fonction :

$$H : \{0, 1\}^* \rightarrow \{0, 1\}^n$$

qui, à partir d'une chaîne de bits quelconque m , produit un haché (condensat ou empreinte) $h = H(m)$ de taille fixe (n bits).

À quoi ça sert ?

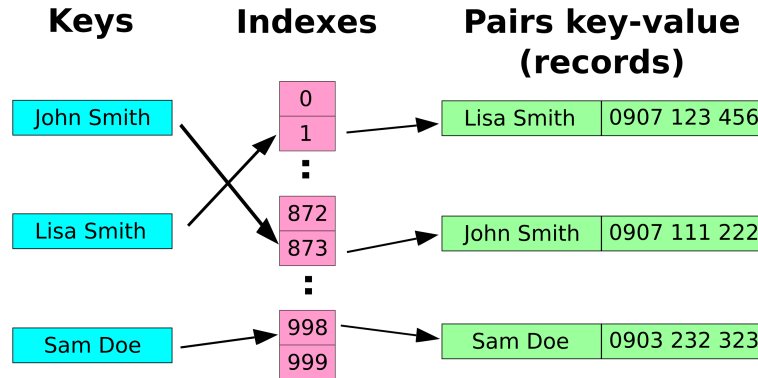


Figure 1. – Un annuaire représenté comme une table de hachage. La fonction de hachage transforme les clés (en bleu) en valeurs de hachage (en rouge) indexant les éléments de la table (alvéoles) composés de paires clé-valeur (en vert). (source Wikipedia)

À quoi ça sert ?(ii)

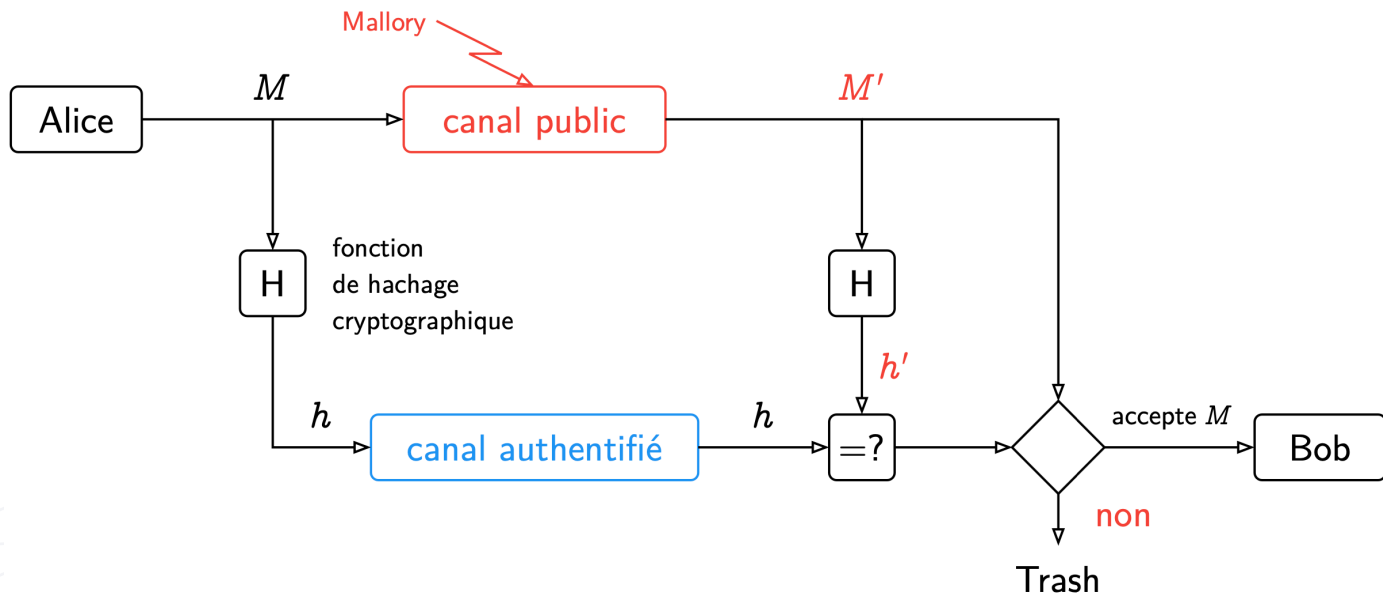


Figure 2. – Vérification de l'intégrité d'un fichier. L'empreinte du fichier téléchargé est calculé puis comparée avec l'empreinte officielle.

À quoi ça sert ?(iii)

Enregistrement des mots de passe !

Condensats Cryptographiques

Une telle **fonction de condensation** est dit **cryptographique** lorsqu'elle vérifie un certain nombre de propriétés :

- **résistance à la pré-image** : pour toute valeur de hachage h , il est difficile de trouver un message m tel que $H(m) = h$.
- **résistance à la seconde pré-image** : pour une valeur m_1 donnée, il est difficile de trouver un message m_2 tel que $H(m_1) = H(m_2)$.
- **résistance aux collisions** : il est difficile de trouver deux message différents m_1 et m_2 tels que $H(m_1) = H(m_2)$. Une telle paire est appelée une collision de hachage cryptographique.