

Considérons une *fonction de compression*  $f : \{0, 1\}^{n+\ell} \rightarrow \{0, 1\}^n$  avec  $\ell \geq 2$  et  $h_0 \in \{0, 1\}^n$  un vecteur d'initialisation (utilisée pour le premier bloc). Nous considérons un processus de remplissage  $\mathcal{R}$  défini sur  $\{0, 1\}^*$  et vérifiant  $|\mathcal{R}(m)| \equiv 0 \pmod{\ell}$  pour tout message  $m \in \{0, 1\}^*$  (*i.e.* qui transforme le message à hacher en un message dont la longueur est un multiple de  $\ell$ ). La valeur de la fonction de hachage itérée  $\mathcal{H}$  construite à partir de  $f$  et  $\mathcal{R}$  est définie par  $\mathcal{H}(m) = f(h_k, m_k)$  où

- la valeur  $\mathcal{R}(m)$  en  $(k + 1)$  blocs de  $\ell$  bits  $\mathcal{R}(m) = (m_0, \dots, m_k) \in (\{0, 1\}^\ell)^k$  ;
- $h_i = f(h_{i-1}, m_{i-1})$  pour tout  $i \in \{1, \dots, k\}$ .

R. MERKLE et I. DAMGÅRD ont montré que si la fonction de compression est résistante aux collisions et si le processus de bourrage est bien construit, alors la fonction de hachage itérée  $\mathcal{H}$  obtenue à partir de  $f$  est résistante aux collisions.

### Exercice 1 : Construction de Merkle-Damgård

**1.a]** Supposons que les messages dont la longueur n'est pas un multiple de la longueur du bloc  $\ell$  sont complétés par une chaîne de zéros jusqu'à ce que la longueur soit un multiple de  $\ell$  (*i.e.* en posant  $i = |m| \pmod{\ell}$ ,  $\mathcal{R}(m) = m \parallel 0^{\ell-i}$ ).

Montrer que la fonction itérée obtenue à partir de  $f$  et  $\mathcal{R}$  n'est pas résistante aux collisions.

**1.b]** Supposons désormais que le processus de bourrage est défini de la façon suivante :

$$\mathcal{R}(m) = m \parallel 10^{\ell-i-1} \text{ avec } i = |m| \pmod{\ell}$$

Montrer que si l'on dispose d'un bloc de message  $z$  tel que  $f(h_0, z) = h_0$  alors il est possible de trouver des collisions pour la fonction itérée obtenue à partir de  $f$  et  $\mathcal{R}$ .

**1.c]** Supposons enfin qu'un dernier bloc contenant la longueur binaire du message est concaténé au procédé de bourrage de la question précédente (*i.e.* en notant  $\tau_m$  un encodage binaire de la longueur  $|m|$  de  $m$ , nous avons  $\mathcal{R}(m) = (m \parallel 10^{\ell-i-1} \parallel \tau_m)$  avec  $i = |m| \pmod{\ell}$ ).

Montrer que la fonction itérée obtenue à partir de  $f$  et  $\mathcal{R}$  est résistante aux collisions si  $f$  est résistante aux collisions.

### Exercice 2 : Multicollisions pour les fonctions de hachage itérées

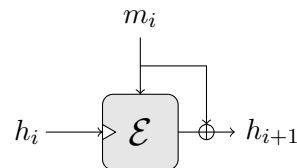
Nous considérons une fonction de hachage  $\mathcal{H} : \{0, 1\}^r \rightarrow \{0, 1\}^n$  construite à partir d'une fonction de compression  $f : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^n$  par la méthode de Merkle-Damgård (avec  $\ell > 2n$ ).

Soit  $\mathcal{H}_c : \{0, 1\}^{c \cdot \ell} \rightarrow \{0, 1\}^n$  une fonction construite à partir de  $f$  par la méthode de Merkle-Damgård mais sans ajouter de bourrage et utilisée uniquement pour les messages de longueur fixe égale à un multiple de  $\ell$ .

**2.a]** En cherchant deux collisions bien choisies pour la fonction de compression, montrer comment obtenir une 4-multicollision pour  $\mathcal{H}_2$ .

**2.b]** Expliquer comment transformer cette 4-multicollision pour  $\mathcal{H}_2$  en une 4-multicollision pour  $\mathcal{H}$ .

**2.c]** Généraliser en montrant qu'on peut obtenir une  $2^t$ -multicollision pour  $\mathcal{H}$  pour le coût de  $t$  collisions sur  $f$ .



Une construction de fonction de compression à partir d'un système de chiffrement par bloc et résistante aux collisions a été proposée par Matyas, Meyer et Oseas. La fonction de compression  $f : \{0, 1\}^n \times \{0, 1\}^\ell \rightarrow \{0, 1\}^n$  est définie par  $f(h, m) = \mathcal{E}_h(m) \oplus m$  où  $\mathcal{E}$  est un système de chiffrement par blocs de  $n$  bits. Il est conjecturé qu'il n'existe aucune attaque plus efficace que les attaques génériques sur cette construction ou sur la construction duale connue sous le nom de construction de Davies-Meyer (*i.e.*, une attaque en collision nécessite environ  $2^{n/2}$  évaluations de la fonction  $f$  et une attaque en (seconde) pré-image nécessite environ  $2^n$  évaluations de la fonction  $f$ ). Cette conjecture a été démontrée sous l'hypothèse que la primitive de chiffrement par bloc utilisée a un comportement idéal. En pratique, les systèmes de chiffrement par bloc n'ont pas les mêmes propriétés que les fonctions aléatoires et l'exercice suivant montre que si le chiffrement par bloc utilisé a des propriétés spécifiques alors la fonction de compression peut ne pas être sûre.

### Exercice 3 : Sécurité de la construction de Matyas-Meyer-Oseas avec le DES

Montrer que la fonction de compression  $f$  n'est pas résistante aux collisions lorsque  $\mathcal{E} = \text{DES}$  dans la construction de Matyas-Meyer-Oseas.

### Exercice 4 : Attaque en collision contre fonctions de hachage concaténées

Soient  $\mathcal{H}_1$  et  $\mathcal{H}_2$  deux fonctions de hachage de même domaine qui produisent des empreintes de  $n$  bits et considérons la fonction de hachage  $\mathcal{H}$  définie pour tout message  $m$  par  $\mathcal{H}(m) = \mathcal{H}_1(m) \parallel \mathcal{H}_2(m)$  (en particulier  $\mathcal{H}$  produit des empreintes de  $2n$  bits).

**4.a]** Montrer que  $\mathcal{H}$  est résistante aux collisions dès que l'une des fonctions  $\mathcal{H}_1$  ou  $\mathcal{H}_2$  est résistante aux collisions.

**4.b]** En supposant que  $\mathcal{H}_1$  est une fonction de hachage itérée vulnérable à l'attaque des multicollisions de l'exercice précédent, proposer un algorithme pour construire une collision pour la fonction  $\mathcal{H}$  en environ  $2^{n/2}(n/2)$  évaluations de la fonction de hachage  $\mathcal{H}_1$  et  $2^{n/2}$  évaluations de la  $\mathcal{H}_2$ .