

Le chiffrement de Merkle-Hellman

Les séquences super-croissantes

Une séquence de nombres est une séquence super-croissante (super-increasing sequence) si chaque nombre de cette séquence est plus grand ou égal à la somme des éléments qui le précèdent dans la séquence.

Le problème de la somme des sous-ensembles (subset sum problem) se résout en une complexité polynomiale pour les séquences super-croissantes (voir l'algorithme dans les transparents).

Soit la séquence super-croissante suivante : $E = \{6, 15, 37, 83, 190, 386, 781, 1580\}$. Existe-t-il un sous-ensemble de E tel que la somme des éléments de sous-ensemble donne $s = 1221$?

L'algorithme évolue ainsi :

$i = 8 = E $	$1221 \geq 1580?$	non $\rightarrow x_8 = 0$
$i = 7$	$1221 \geq 781?$	oui $\rightarrow x_7 = 1$ et $s = 440$
$i = 6$	$440 \geq 386?$	oui $\rightarrow x_6 = 1$ et $s = 54$
$i = 5$	$54 \geq 190?$	non $\rightarrow x_5 = 0$
$i = 4$	$54 \geq 83?$	non $\rightarrow x_4 = 0$
$i = 3$	$54 \geq 37?$	oui $\rightarrow x_3 = 1$ et $s = 17$
$i = 2$	$17 \geq 15?$	oui $\rightarrow x_2 = 1$ et $s = 2$
$i = 1$	$2 \geq 6?$	non $\rightarrow x_1 = 0$

Quand la boucle de l'algorithme se termine s vaut toujours 2 (et non 0), cela indique qu'il n'y a pas de sous-ensemble de valeurs de E telles que leur somme égale s . En effet, si nous prenons les éléments de E correspondant au x_i qui valent 1, nous avons : $781 + 386 + 37 + 15 = 1219 \neq 1221$.

Si avec la même séquence E , nous cherchons un sous-ensemble dont la somme serait $s = 619$, alors nous avons :

$i = 8 = E $	$619 \geq 1580?$	non $\rightarrow x_8 = 0$
$i = 7$	$619 \geq 781?$	non $\rightarrow x_7 = 0$
$i = 6$	$619 \geq 386?$	oui $\rightarrow x_6 = 1$ et $s = 233$
$i = 5$	$233 \geq 190?$	oui $\rightarrow x_5 = 1$ et $s = 43$
$i = 4$	$43 \geq 83?$	non $\rightarrow x_4 = 0$
$i = 3$	$43 \geq 37?$	oui $\rightarrow x_3 = 1$ et $s = 6$
$i = 2$	$6 \geq 15?$	non $\rightarrow x_2 = 0$
$i = 1$	$6 \geq 6?$	oui $\rightarrow x_1 = 1$ et $s = 0$

Quand la boucle de l'algorithme se termine s vaut 0 ce qui signifie que nous avons trouvé un sous-ensemble de valeurs de E telles que leur somme égale s . Si nous prenons les éléments de E correspondant au x_i qui valent 1, nous avons : $386 + 190 + 37 + 6 = 619$.

Exemple du chiffrement Merkle-Hellman

Soient les informations suivantes relatives à Bob :

- $n = 9$;
- $(b_1, \dots, b_9) = (2, 5, 9, 21, 45, 103, 215, 450, 946)$ une suite supercroissante ;
- $M = 2003$;
- $W = 1289$ (le $\text{pgcd}(W, M) = 1$).

Nous avons $(a_1, \dots, a_9) = (575, 436, 1586, 1030, 1921, 569, 721, 1183, 1570)$ qui n'est plus une suite super-croissante.

Si Alice veut envoyer le message $x = 101100111$ à Bob, elle calcule

$$y = 575 + 1586 + 1030 + 721 + 1183 + 1570 = 6665$$

Pour déchiffrer Bob calcule

$$d = W^{-1}y \pmod{M} = (1289)^{-1}6665 = 3176665 = 1643 \pmod{2003}$$

Puis Bob cherche les x_i tel que :

$$s = \sum_{i=1}^n x_i b_i$$

$$s = 1643 \rightarrow x_9 = 1 \rightarrow s = 697 \rightarrow x_8 = 1 \rightarrow s = 247 \rightarrow x_7 = 1 \rightarrow s = 32 \rightarrow x_6 = 0, x_5 = 0, x_4 = 1 \rightarrow s = 11 \rightarrow x_3 = 1 \rightarrow s = 2 \rightarrow x_2 = 0, x_1 = 1 \rightarrow s = 0$$

Et il retrouve $x = 101100111$