6. La signature numérique

Les activités humaines reposent pour beaucoup sur la confiance dans les engagements que contractent les différents acteurs entre eux. Cette confiance se matérialise par une signature apposée à un document. Il a fallu trouver un équivalent numérique de la signature, produite par une personne particulière et vérifiable par tous.

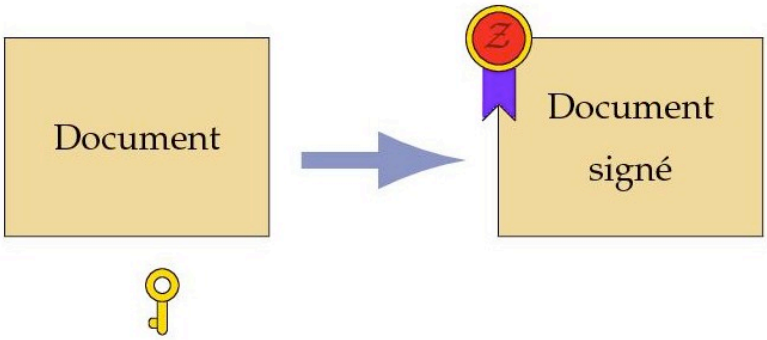

Fig. 3.6 Signature à clé publique : La production de la signature nécessite une clé privée et change à chaque document. Sa vérification ne requiert qu'une clé publique accessible à tous.

Un mécanisme à clé publique comme le RSA autorise la production d'une telle signature numérique. Il suffit, pour s'engager, d'élever le document qu'on souhaite signer à la puissance exposant privé modulo *n*. Le résultat constituera la signature du document. Quiconque pourra vérifier la signature en l'élevant à la puissance exposant public modulo *n*, mais personne ne pourra produire la signature sans la connaissance de l'exposant privé.

Cette exemple de la signature RSA qui consiste en fait à un chiffrement avec la clé privée ont conduit les chercheurs à se demander si cette propriété était dans la nature de la notion de signature. La signature est-elle duale du chiffrement à clé publique. La réponse est négative. Il n'est pas nécessaire de disposer d'une fonction à sens unique avec trappe pour réaliser ce mécanisme. Une simple fonction à sens unique sans trappe suffit. Une fonction est dite *à sens unique* si elle est facilement calculable, mais étant donnée une valeur, il est pratiquement impossible de trouver un paramètre qui donnera ce résultat.

Par exemple, pour un nombre premier *p*, il est facile d'élever n'importe quel nombre à la puissance *n* modulo *p* avec une succession de multiplications et d'élévations au carré. Mais retrouver l'exposant *n* à partir du résultat est un problème qu'on ne sait pas résoudre de manière efficace aujourd'hui. Ce problème s'appelle le problème du logarithme discret.

Pour signer un document avec une fonction à sens unique, il suffit de disposer d'une clé secrète constituée de deux couples de valeurs $x_1 ... x_n$ et $y_1 ... y_n$. La clé publique correspondante est constituée par les images $a_i = f(x_i)$ et $b_i = f(yi)$ par une fonction à sens unique *f*. Pour signer un message

$m = m_1...m_n$ où chaque m_i est une information binaire valant 0 ou 1, j'appose au message la révélation des données x_i si m_i vaut 0 et y_i si m_i vaut 1. Le destinataire pourra aisément vérifier, grâce à la clé publique, que $f(x_i) = a_i$ si m_i vaut 0 et $f(y_j) = b_j$ si m_i vaut 1. Comme la fonction est à sens unique, il sera difficile à un adversaire de révéler des valeurs convenables en l'absence de la connaissance des paramètres x_i et $y_{i.}$.

Cette signature n'a qu'un intérêt théorique en raison de sa totale inefficacité. La signature d'un document est bien plus grande que le document lui-même et la clé privée n'est pas réutilisable pour un autre document. Mais l'intérêt théorique est fondamental : la signature numérique peut se construire à partir d'une fonction à sens unique. Il n'y a pas besoin de trappe pour signer un document.