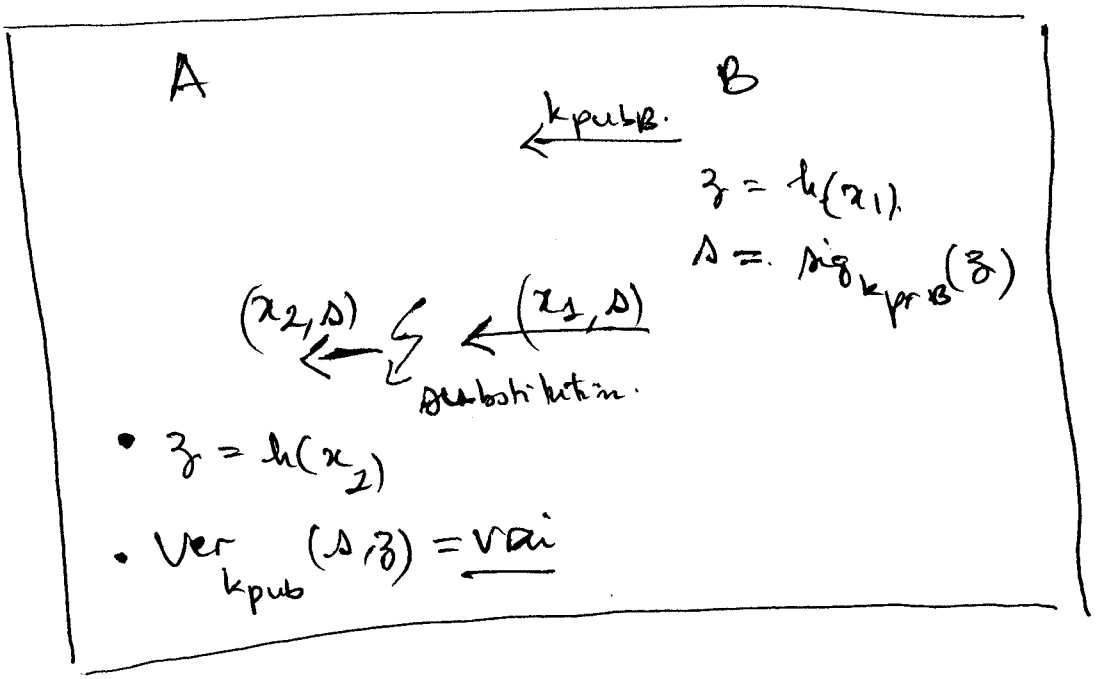
(2) Etant donné $h(x_1) = z$, il est difficile de trouver x_2 tq. $h(x_2) = z$. (Collision faible).

Supposons que Bob hache x_1 et signe $h(x_1)$.

Supposons que O peut trouver x_2 avec $h(x_1) = h(x_2)$:



(3) Collision forte : h est fortement résistante au collision, s'il est difficile de trouver x_1, x_2 tq $h(x_1) = h(x_2)$. Cette propriété est plus difficile que (2). A la base de cette propriété, O peut attaquer :